ISSN : 2229 - 3515

Volume : 9 ,
Special Issue of NCSCCSS 2019
22-23rd November 2019

Proceedings of the
2nd National Conference
on
Soft Computing, Communication Systems & Sciences

(NCSCCSS 2K19)

22-23rd November 2019

International Journal of ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief
Dr.C.Srinivasa Kumar

Organized by

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

Convener

Dr. Kanaka Durga Returi

Dr.A.Praveen Kumar

Published by
BHAVANA RESEARCH CENTER

2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES

(NCSCCSS 2K19)

on

22-23rd November 2019

Conveners

Dr. KANAKA DURGA RETURI

Dr. ARCHEK PRAVEEN KUMAR

Organized by

Department of Computer Science & Engineering
Department of Electronics & Communication Engineering
MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN
Maisammaguda, Medchal, Hyderabad-500100, TS, INDIA

The Organizing Committee is not responsible for the statements made or opinions expressed in the papers included in the volume.

Sri. CH. MALLA REDDY
M.L.A -Medchal
Hon'ble Minister, Govt. of Telangana
Labour & Employment, Factories,
Women and Child Welfare.
Founder Chairman, MRGI

Message

MRCEW, HYDERABAD has always been a front runner to organize such events and this time too we have come up with “2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K19) on 22-23rd November 2019”. *I* strongly believe that this conference will provide tools and knowledge to overcome significant problems appearing in our industry and society by identifying innovative ideas and technologies introduced by the researchers and students. The success of this conference will encourage us in introducing many more initiatives for innovative trends in the coming years.

CH. MALLA REDDY

Sri. CH.MAHENDER REDDY

Secretary, MRGI

Message

It gives me immense pleasure to be a part of this hosting team of "2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K19)". I hope that the conference serves as a locus for interdisciplinary, a space for discourse and collaboration. I would like to express my appreciation to the organizing committee for their dedicated efforts to materialize the conference. I hope all the participants will have a fruitful and beneficial experience. Finally, I congratulate Principal, HODs, college faculty, student representatives and participant for their efforts in organizing and participating in this conference and wish the conference all the success.

Sri. CH.MAHENDER REDDY

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.
E-Mail: rg.mrcew@gmail.com

EAMCET CODE:
MREW
JNTUH CODE: RG

DR. VAKA MURALI MOHAN
B. Tech., M.Tech (ChE)., Ph.D (AU)
M.Tech (CSE)., Ph.D (GU)
MISTE., MCSI., MSAI., MIEEE., MUACEE
PRINCIPAL & PROFESSOR of CSE
murali_vaka@yahoo.com

Message

I am very happy that the Department of CSE & ECE is organizing "2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K19)". This conference is a unique forum for exchange of innovative ideas, technical expertise for technological advancements etc. in this evergreen field. It includes keynote address from Academicians and paper presentation by research scholars. It is a matter of joy for us to welcome the participants to this conference. In a nutshell, the conference promises to transcend to a new and unprecedented level of excellence. I congratulate the all faculty members of CSE & ECE for their cooperation and hard work in making this conference a grand success.

DR. VAKA MURALI MOHAN

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.
E-Mail: rg.mrcew@gmail.com

EAMCET CODE: MREW
JNTUH CODE: RG

DR. KANAKA DURGA RETURI
B. Tech., M.Tech., Ph.D
HOD & PROFESSOR of CSE

CONVENER

Message

It is our great honor to welcome you all the delegates from various parts of the Country to 2nd National Conference on Soft Computing, Communication Systems & Sciences (NCSCCSS 2K19). Information provided in various papers and reproduced in the proceedings is aimed at benefiting the Engineers and professionals. It is expected that the purpose would be served in a satisfactory manner through in-depth discussion and interaction among participants during the conference. I take this opportunity to record my heartfelt appreciation and gratitude to all the authors, delegates, conference chairman and all others participating. We sincerely hope that NCSCCSS 2K19 provides an excellent open forum to exchange ideas and latest research accomplishments among academia and industries.

DR. KANAKA DURGA RETURI

MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN

(Approved by AICTE, New Delhi & Affiliated to JNTU, Hyderabad)

An ISO 9001: 2015 certified Institution

Maisammaguda, Gundlapochampally (V), Medchal (Mdl & Dist) -500100, Telangana.
E-Mail: rg.mrcew@gmail.com

EAMCET CODE:
MREW
JNTUH CODE: RG

DR. ARCHEK PRAVEEN KUMAR
B. Tech., M.E., Ph.D
HOD & PROFESSOR of ECE

CONVENER

Message

It is our great honour to welcome you all the delegates from various parts of the Country to "2nd National Conference on Soft Computing, Communication Systems & Sciences (NCSCCSS 2K19)". The proceedings represent scholarly work of advanced and innovative thinkers and educators from around the world. It is felt that it is only through the exchange of information that one can hope to keep up with the rapidly changing world around us. I wish all the delegates, a great educational and informative experience at the conference. My best wishes to all the participants of this conference.

DR. ARCHEK PRAVEEN KUMAR

INTERNATIONAL JOURNAL OF ADVANCES IN SOFTCOMPUTING TECHNOLOGY

(ISSN NO: 2229-3515)

(Published by **BHAVANA RESEARCH CENTER, HYDERABAD**)

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY
BHAVANA RESEARCH CENTER

DR. C.SRINIVASA KUMAR
M.Sc., Ph.D (SVU), M.Tech (CSE)., Ph.D (GU)
MISTE, MCSI MISTE., MCSI., MSAI
EDITOR–IN–CHIEF

MESSAGE

I am glad to note that "MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN" has taken the initiative to conduct a two day 2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K19) on 22-23rd November 2019. Advances in Soft Computing & Communication Technologies gives the latest communication promises faster than other facilities, because of the best possible information and communication updates in current trends. I am sure the deliberations during the conference will expose the Staff, Research Scholars and Students to what is new and what is ahead in Soft Computing & Communication Technologies..........

I congratulate the organizers and convey my best wishes for the success of the Conference in the fulfillment of its objectives.

With Regards

(DR. C.SRINIVASA KUMAR)
Editor-In-Chief, IJASCT

2nd NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES

(NCSCCSS 2K19)

on

22-23rd November 2019

Chief Patron

Sri. CH. MALLA REDDY	Founder Chairman, Malla Reddy Group of Institutions

Patron

Sri. CH. MAHENDER REDDY	Secretary, Malla Reddy Group of Institutions
Dr. CH. BHADRA REDDY	President, Malla Reddy Group of Institutions
Dr. VAKA MURALI MOHAN	Principal, MRCEW

Convener

Dr. Kanka Durga Returi	Professor & HOD, CSED
Dr. Archek Praveen Kumar	Professor & HOD, ECED

International Advisory Committee

Dr. Ahamad J Rusumdar	KIT, Germany
Dr. V.R.Chirumamilla	EUT, Netherlands
Dr. Silviya Popova	ISER, BAS, Bugaria
Dr. Shaik Feroz	CCE, Oman
Dr. Lean Yu	AMSC, Beijing, China
Dr. Mohen Hayati	RU, Iran
Dr. Kun-Lin Hsiesh	NTU, Taiwan
Dr. Ghazali Bin Sulong	UT, Malaysia
Dr. Halis Altun	MU, Turkey

Technical Committee

Dr.A.Vinay Babu	JNTU Hyderabad
Dr.J.A.Chandulal	GU, Visakhapatnam
Dr.P. Premchand	OU, Hyderabad
Dr. G. Hemanth Kumar	UM, Mysore
Dr.M. Srinivasa Rao	SIT, JNTU Hyderabad
Dr.A.Damodaram	SVU Tirupathi
Dr.G.Govardhan	JNTU Hyderabad
Dr.P.R.K.Murti	Rtd, HCU Hyderabad
Dr. Doreswamy	UM, Mangalore
Dr. M. V. Satish Kumar	TCU, Assam
Dr. J.K. Mantri	NOU, Orissa

Advisory Board

Dr. D. Rajya Lakshmi	JNTU Kakinada
Dr. V. Kamakshi Prasad	JNTU Hyderabad
Dr. G. Narasimha	JNTU Jagityal
Dr. P. V.Nageswara Rao	GU, Visakhapatnam
Dr. B. Padmaja Rani	JNTU Hyderabad
Dr.Md.Zafir Ali Khan	IIT Hyderabad
Dr. N. Kalyani	GNITS, Hyderabad
Prof. K. Srujan Raju	CMRTC & CSI Hyderabad
Mr.Anirban Pal	Tech Mahindra, Hyderabad
Mr.Gautham Mahapatra	Sr.Scientist

****

ISSN: 2229-3515

INTERNATIONAL JOURNAL OF ADVANCES IN
SOFT COMPUTING TECHNOLOGY

BHAVANA RESEARCH CENTER
#A-905, 2nd Floor, Allwyn Colony, Phase-2,
Kukatpally, Hyderabad – 500 072, TS, India
☎.: 91- 7730883888
✉ :editor@ijasct.in, brchyd_2010@yahoo.com
www.ijasct.in

ISSN: 2229-3515

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY

Volume: 09 *Special Issue of NCSCCSS 2K19* *22 – 23rd NOVEMBER, 2019*

PERFORMING LEXICAL ANALYSIS COMBINING WORDS AND SENTENCES

Venkata Krishna Mohan Chavali[1]., K.Spandhana[2]., Bolla Pooja[3]., B.Priya Nayani[4] ., G.Sanvitha[5]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- chvkm@rediffmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0543, 16RG1A0508, 16RG1A0510, 16RG1A0528),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract*— We develop numerous neural systems with tailoring loss functions to understand sentiment embeddings. We learn sentiment embeddings from tweets with good and bad emoticons as distant-supervised corpora with no manual annotations. Within this paper, we advise learning sentiment-specific word embeddings dubbed sentiment embeddings for sentiment analysis. An upright forward strategy is to represent each word like a one-hot vector, whose length is vocabulary size and just one dimension is 1, with all of others being . To be able to learn sentiment embeddings effectively, we develop numerous neural systems to capture sentiment of texts in addition to contexts of words with dedicated loss functions. We collect sentence level sentiment information instantly from Twitter. This is dependent on the glory that bigger training data usually results in more effective word representation. To guarantee the excellence of the expanded words, we set threshold for every category to gather the products rich in quality as expanded words. We evaluate the potency of sentiment embeddings empirically by making use of these to three sentiment analysis tasks. Existing embedding learning approaches are mainly based on distributional hypothesis. However, it might be a tragedy for sentiment analysis because they have opposite sentiment polarity labels.

***Keywords*— Sentiment embeddings, natural language processing, word embeddings, sentiment analysis, neural networks.**

1. INTRODUCTION

We advise learning sentiment embeddings that encode sentiment of texts in continuous word representation. Sentiment embeddings could be naturally utilized as word features for various sentiment analysis tasks without feature engineering. We apply sentiment embeddings to word-level sentiment analysis, sentence level sentiment classification, and building sentiment lexicons. A pioneered work in this subject is offered by Bengio et al [1]. They introduce a neural probabilistic language model that learns concurrently a continuing representation for words and also the probability function for word sequences according to these word representations. One common method of uncover the similarities between words would be to become familiar with a clustering of words. Each word is connected having a discrete class, and words within the same class offer a similar experience in certain respects. CBOW model predicts the present word in line with the embeddings of their context words, and Skip-gram model predicts surrounding words because of the embeddings of current word [2].

2. LEARNING METHOD:

Existing embedding learning approaches are mainly based on distributional hypothesis, which claims that the representations of test is reflected by their contexts. Consequently, words concentrating on the same grammatical usages and semantic meanings, for example “hotel” and “motel”, are mapped into neighboring vectors within the embedding space. Since word embeddings capture semantic similarities between words, they've been leveraged as inputs or extra word features for various natural language processing tasks. Mnih and Hinton introduce a log-bilinear language model. Collobert and Weston train word embeddings having a ranking-type hinge loss function by replacing the center word inside a window having a at random selected one. Mikolov et al. introduce continuous bag-of-words (CBOW) and continuous skip-gram, and release the most popular word2vec3 toolkit. CBOW model predicts the present word in line with the embeddings of their context words, and Skip-gram model predicts surrounding words because of the embeddings of current word. Mnih and Kavukcuoglu accelerate the embedding learning procedure with noise contrastive estimation [3]. Disadvantages of existing system: Probably the most serious issue of context-based embedding learning algorithms is they only model the contexts of words but disregard the sentiment information of text. Consequently, words with opposite polarity, for example negative and positive, are mapped into close vectors within the embedding space. Existing word embedding learning algorithms typically just use the contexts of words but disregard the sentiment of texts.

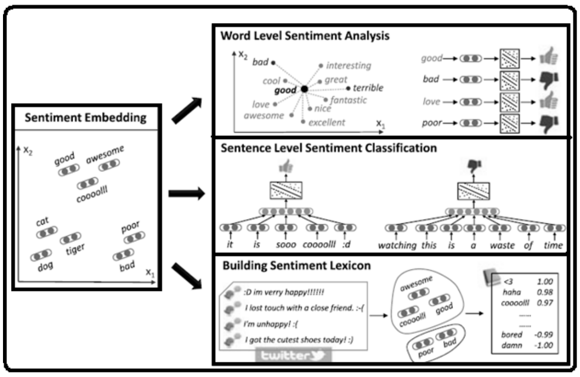


Fig.1.System framework

3. SENTIMENT LEARNING EMBEDDINGS:

Within this paper, we advise learning sentiment-specific word embeddings dubbed sentiment embeddings for sentiment analysis. We retain the potency of word contexts and exploit sentiment of texts for learning more effective continuous word representations. By recording both context and sentiment level evidences, the closest neighbors within the embedding space are not only seen semantically similar but additionally favor to achieve the same sentiment polarity, that it is in a position to separate negative and positive to opposite ends from the spectrum. We learn sentiment embeddings from tweets, leveraging good and bad emoticons as pseudo sentiment labels of sentences without manual annotations. We have lexical level sentiment supervision from Urban Dictionary with different small listing of sentiment seeds with minor manual annotation. We advise learning sentiment embeddings that encode sentiment of texts in continuous word representation. We learn sentiment embeddings from tweets with good and bad emoticons as distant-supervised corpora with no manual annotations. We verify the potency of sentiment embeddings by making use of these to three sentiment analysis tasks. Empirical experimental results reveal that sentiment embeddings outshine context-based embeddings on several benchmark datasets of those tasks [4]. Benefits of suggested system: We evaluate the potency of sentiment embeddings empirically by making use of these to three sentiment analysis tasks. Word level sentiment analysis on benchmark sentiment lexicons might help us decide if sentiment embeddings are helpful to uncover similarities between sentiment words. Sentence level sentiment classification on tweets and reviews allow us to understand whether sentiment embeddings are useful in recording discriminative features for predict the sentiment of text. Building sentiment lexicon is helpful for calculating the level that sentiment embeddings improve lexical level tasks that should find similarities between words. Experimental results reveal that sentiment embeddings consistently beat context-based word embeddings, and yields condition-of-the-art performances on several benchmark datasets of those tasks.

Implementation: We develop a conjecture model similar towards the representative “context prediction” neural language model provided by Bengio et al. Labutov and Lipson re-embed existing word embeddings with logistic regression by regarding sentiment supervision of sentences like a regularization item. we describe a conjecture model along with a ranking model to encode contexts of words for learning word embeddings. These context-based models is going to be naturally added to sentiment-specific models for learning sentiment embeddings. The contexts of the target word might be preceding, following or surrounding words happened in a bit of text. We describe two neural systems together with a conjecture model along with a ranking model to consider factors of sentiment of sentences [5]. The fundamental concept of the conjecture model is regarding sentiment conjecture like a multi-class classification task. We design a hybrid loss function that is weighted straight line mixture of the sentiment loss and also the context loss. We use 2 kinds of lexical level information, namely word-word associations and word-sentiment associations. We develop two regularizes to naturally incorporate them into aforementioned sentiment, context and hybrid neural models. Within this work, the term clusters utilized in this part are acquired instantly from Urban Dictionary. To be able to collect sources that contains massive word associations, we leverage Urban Dictionary without needing any manual annotation.

Sentiment Analysis at Word-Level: A much better sentiment embedding should be capable of map positive words into close vectors, to map negative words into close vectors, and also to separate positive words and negative words apart. We utilize CBOW within the experiments that is similar to the context-conjecture model. Two hybrid models yields best performances because they capture not just contexts of words but additionally sentiment information of sentences. Because we evaluate sentiment embeddings on word level sentiment analysis lexicons, we don't match up against the embeddings learned with word level information for fair comparison within this part. On word level sentiment analysis, we reveal that sentiment embeddings are helpful for finding similarities between sentiment words [6].

Sentiment Catalog at Sentence-Level: Rather of utilizing hands-crafting features, we use sentiment embeddings to write the feature of the sentence. The sentiment classifier is made from sentences with by hand annotated sentiment polarity. It's important to note that, Twitter sentiment classification evaluation in SemEval asks participants to complete ternary classification over positive, negative and neutral groups. Sentiment embeddings may also be naturally given with other semantic composition models like Recursive Neural Network and Convolution Neural Network. In sentiment analysis community, SVM classifier with bag of ngrams is really a standard baseline for sentiment classification. On sentence level sentiment classification, sentiment embeddings are useful in recording discriminative features for predicting the sentiment of sentences.

Sentiment Lexicon: We introduce a classification method of build sentiment lexicon by regarding sentiment embeddings as word features, after which describe experimental settings and also the results. We evaluate the potency of sentiment lexicons by making use of them as features for Twitter sentiment classification inside a condition-of-the-art supervised learning pipeline [7]. On lexical level task like building sentiment lexicon, sentiment embeddings are proven to become helpful for calculating the similarities between words.

4. CONCLUSION:

Probably the most serious issue of context-based embedding learning algorithms is they only model the contexts of words but disregard the sentiment information of text. By mixing context and sentiment level evidences, the closest neighbors in sentiment embedding space are semantically similar also it favors words with similar sentiment polarity. To be able to learn sentiment embeddings effectively, we develop numerous neural systems with tailoring loss functions, and collect massive texts instantly with sentiment signals like emoticons because the training data. The fundamental concept of ranking model is when the gold sentiment polarity of the word sequence is positive, the predicted positive score ought to be greater compared to negative score. We conduct word level sentiment classification to help investigate the potency of sentiment embeddings in recording similarities between sentiment words. We compare sentiment embeddings with several baseline embedding learning algorithms for Twitter sentiment classification. The potency of sentiment embeddings are verified empirically on three sentiment analysis tasks.

REFERENCES:

[1] Duyu Tang, Furu Wei, Bing Qin, Nan Yang, Ting Liu, and Ming Zhou, "Sentiment Embeddings with Applicationsto Sentiment Analysis", ieee transactions on knowledge and data engineering, vol. 28, no. 2, february 2016.

[2] R. Socher, A. Perelygin, J. Wu, J. Chuang, C. D. Manning, A. Ng, and C. Potts, "Recursive deep models for semantic compositionality over a sentiment treebank," in Proc. Conf. Empirical Methods Natural Lang. Process., 2013, pp. 1631–1642.

[3] A. Mnih and G. Hinton, "Three new graphical models for statistical language modelling," in Proc. 24th Int. Conf. Mach. Learning, 2007, pp. 641–648.

[4] N. Yang, S. Liu, M. Li, M. Zhou, and N. Yu, "Word alignment modeling with context dependent deep neural network," in Proc. 51st Annu. Meeting Assoc. Comput. Linguistics, 2013, pp. 166–175.

[5] P. Nakov, S. Rosenthal, Z. Kozareva, V. Stoyanov, A. Ritter, and T. Wilson, "Semeval-2013 task 2: Sentiment analysis in twitter," in Proc. Int. Workshop Semantic Eval., 2013, vol. 13, pp. 312–320.

[6] M. Baroni, G. Dinu, and G. Kruszewski, "Don't count, predict! A systematic comparison of Context-counting vs. Context-predicting semantic vectors," in Proc. 52nd Annu. Meeting Assoc. Comput. Linguistics, 2014, pp. 238–247.

[7] K. Gimpel, N. Schneider, B. O'Connor, D. Das, D. Mills, J. Eisenstein, M. Heilman, D. Yogatama, J. Flanigan, and N. A. Smith, "Part-of-speech tagging for twitter: Annotation, features, and experiments," in Proc. Annu. Meeting Assoc. Comput. Linguistics, 2011, pp. 42–47.

BALANCING TRADE-OFFS IN MERGE ARTICULATED CONDUIT AND REVERSE FORCE NAVIGATION

Dr.Nelson Jaladanki[1]., A. Ruchitha[2]., D Sai Amrutha[3]., D. Rohini[4] ., L.Rakshitha Reddy[5]

1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- drjenelson.mrcew@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0501, 16RG1A0514, 16RG1A0516, 16RG1A0557),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract*— In comparison, you are able to that the opportunistic variant of backpressure, diversity backpressure routing ensures bounded expected total backlog for those stabilizable arrival rates. D-ORCD with single destination is demonstrated to make sure a bounded expected delay for those systems and under any admissible traffic, as long as the speed of computations is sufficiently fast in accordance with traffic statistics. Opportunistic routing mitigates the outcome of poor wireless links by exploiting the broadcast nature of wireless transmissions and also the path diversity. E-DIVBAR is suggested: when selecting the following relay one of the groups of potential forwarders, E-DIVBAR views the sum differential backlog and also the expected hop-count towards the destination. The present property of ignoring the price towards the destination, however, becomes the bane of the approach, resulting in poor delay performance in low to moderate traffic. The primary contribution of the paper is to supply a distributed opportunistic routing policy with congestion diversity to which, rather of the simple addition utilized in E-DIVBAR, the congestion details are integrated using the distributed shortest path computations. We reveal that an identical analytic guarantee could be acquired concerning the throughput optimality of D-ORCD. Particularly, we prove the throughput optimality of D-ORCD by searching in the convergence of D-ORCD to some centralized form of the formula.

***Keywords*— Stabilizable, congestion measure, Lyapunov analysis, opportunistic routing, queuing stability, routing policy**

1. INTRODUCTION

We think about the problem of routing packets across a multi-hop network composed of multiple causes of traffic and wireless links while making certain bounded expected delay. Each packet transmission could be overheard with a random subset of receiver nodes among that the next relay is chosen opportunistically. When multiple streams of packets will be to traverse the network, however, it may be desirable to route some packets along longer or even pricier pathways, if these pathways eventually result in links which are less congested [1]. More precisely, the opportunistic routing decisions come in a web-based manner by selecting the following relay in line with the actual transmission outcomes in addition to a rank ordering of neighboring nodes. To make sure throughput optimality, backpressure-based algorithms make a move completely different. This very property of ignoring the price towards the destination, however, becomes the bane of the approach, resulting in poor delay performance in low to moderate traffic. E-DIVBAR is suggested: when selecting the following relay one of the groups of potential forwarders, E-DIVBAR views the sum differential backlog and also the expected hop-count towards the destination. The primary contribution of the paper is to supply a distributed opportunistic routing policy with congestion diversity (D-ORCD) to which, rather of the simple addition utilized in E-DIVBAR, the congestion details are integrated using the distributed shortest path computations. We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed QualNet simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality. Within this work, however, we've selected to concentrate our comparative analysis around the following solutions in literature that have similar overhead, complexity, and practical structure: ExOR, DIVBAR, and E-DIVBAR. Under this insurance policy packets are routed based on a rank ordering from the nodes with different congestion measure [2]. In addition, we suggested an operating distributed and asynchronous 802.11 compatible implementation of D-ORCD, whose performance was investigated using a detailed group of QualNet simulations for practical and realistic systems. The primary challenge in the style of minimum-delay routing policies is balancing the trade-off between routing the packets across the shortest pathways towards the destination and disbursing the traffic based on the maximum backpressure. Compared, D-ORCD may very well be a packet-based form of the min-backlogged-path routing without an excuse for the enumeration of pathways over the network and/or pricey computations of total backlog along pathways. In addition, this paper proposes an operating implementation of D-ORCD which empirically optimizes critical formula parameters as well as their effects on delay in addition to protocol overhead. In addition, while LIFO-Backpressure policy guarantees stability with minimal queue-length variations, realistic burst traffic in large multi-hop wireless systems may lead to queue-length variations and unnecessarily high delay.

2. CLASSICAL DESIGN:

The opportunistic routing schemes could possibly cause severe congestion and unbounded delay. In comparison, you are able to that the opportunistic variant of backpressure, diversity backpressure routing ensures bounded expected total backlog for those stabilizable arrival rates. To make sure throughput optimality, backpressure-based algorithms make a move completely different: instead of using any metric of closeness towards the destination, they pick the receiver using the largest positive differential backlog [3]. Disadvantages of existing system: Other existing provably throughput optimal routing policies distribute the traffic in your area inside a manner much like DIVBAR and therefore, lead to large delay. E-DIVBAR doesn't always create a better delay performance than DIVBAR.

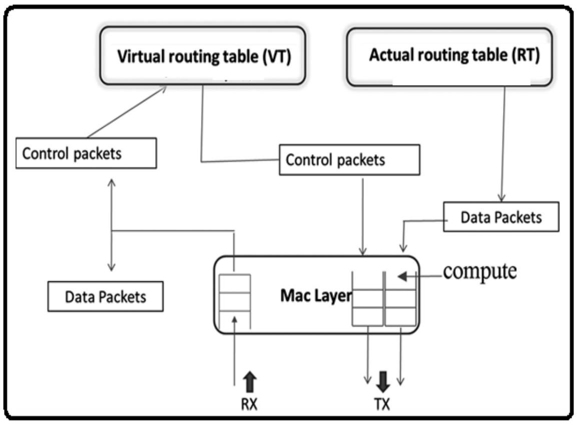


Fig.1.Proposed block diagram

3. ROBUST SCHEME:

An extensive analysis from the performance of D-ORCD is supplied in 2 directions: We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination (single commodity) and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality [4]. Throughout the transmission stage, a node transmits a packet. Within this paper, we provided a distributed opportunistic routing policy with congestion diversity by mixing the key facets of shortest path routing with individuals of backpressure routing. Simulations demonstrated that D-ORCD consistently outperforms existing routing algorithms. Benefits of suggested system: We reveal that D-ORCD exhibits better delay performance than condition-of-the-art routing policies concentrating on the same complexity, namely, ExOR, DIVBAR, and E-DIVBAR. We reveal that the relative performance improvement over existing solutions, generally, depends upon the network topology but is frequently significant used, where perfectly symmetric network deployment and traffic the weather is uncommon. The optimality from the centralized option would be established using a type of Lyapunov functions suggested.

Implementation: Throughout the acknowledgment stage, each node which has effectively received the transmitted packet, transmits an acknowledgment towards the transmitter node. D-ORCD then takes routing decisions with different congestion-aware distance vector metric, known as the congestion measure. D-ORCD uses routing table each and every node to look for the next best hop. The routing table at node includes a listing of neighbors along with a structure composed of believed congestion measure for those neighbors in connected with various destinations. The routing table functions like a storage and decision component in the routing layer. The temporary congestion measures are computed inside a fashion much like a distributed stochastic routing computation of utilizing the backlog information at the outset of the computation cycle. More precisely, node periodically computes its very own congestion measure and subsequently advertises it to the neighbors using control packets at times of seconds. More particularly, throughout the relaying stage, the relaying responsibility from the packet is now use a node using the least congestion measure among those that have obtained the packet. The congestion way of measuring a node connected having a given destination provides approximately the perfect draining duration of a packet coming at this node until it reaches destination. Finally the particular routing table is updated while using records within the virtual routing table after every second [5]. Noting the expected transmission time at node for that packet may then be approximated. We discuss the implementation problems with D-ORCD, especially, distributed and asynchronous iterative Computations. We offer a short discussion from the fundamental challenges of D-ORCD such as the three-way handshake procedure employed in the MAC layer, link quality estimation, avoidance of loops while routing, and overhead reduction issues. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively. One of the leading challenges within the implementation of the opportunistic routing formula, generally, and D-ORCD particularly, is the style of an 802.11 compatible acknowledgement mechanism in the MAC layer. Here we propose an operating and straightforward method to implement acknowledgement architecture. Specifically, before any transmission, transmitter performs funnel sensing and starts transmission following the back off counter is decremented to zero. The priority ordering determines the virtual time slot where the candidate nodes transmit their acknowledgement [6]. Nodes within the set which have effectively received the packet then transmit acknowledgement packets sequentially within the order based on the transmitter node. Within our implementation, we've cheated the priority-based queuing D-ORCD prioritizes the control packets by assigning them the greatest strict priority, lowering the probability the packets are delivered to the MAC layer as well as making certain a prompt receiving the control packets. Furthermore, D-ORCD scheduler assigns a sufficiently lower PHY rate for that control packets. In passive probing, the overhearing capacity from the wireless medium is required. The nodes are configured to promiscuous mode, hence enabling these to hear the packets from neighbors. In passive probing, the MAC layer monitors the amount of packets caused by the neighbors such as the retransmissions. We've extended the rule to D-ORCD by advertising the routes as unreachable to greater rated nodes. Particularly, you can easily observe that this overhead cost, i.e., the entire quantity of ACKs sent per data packet transmission, increases linearly with how big the group of potential forwarders. Thus, we think about a modification of D-ORCD by means of opportunistically routing with partial diversity [7]. We think about the modifications of D-ORCD with partial diversity and choose the amount of neighbors which acknowledge the reception from the packet. This analysis characterizes the trade-off between performance and also the overhead cost connected with receiver diversity. In Split-horizon with poison reverse, a node advertises routes as unreachable towards the node by which these were learned. Without effort, this process penalizes the routes with loops and removes them in the group of available alternatives. Finally, a weighted average can be used to mix the active and passive estimates to look for the link success odds.

3. CONCLUSION:

The aim of this paper would be to design a routing policy with improved delay performance over existing opportunistic routing policies. We advise a period-different distance vector, which helps the network to route packets via a neighbor using the least believed delivery time. D-ORCD opportunistically routes a packet using three stages of: transmission, acknowledgment, and relaying. We provided theoretical throughput optimality evidence of D-ORCD. In D-ORCD, we don't model the interference in the nodes within the network, but rather leave that issue to some classical MAC operation. Passive probing doesn't introduce any extra overhead cost but could be slow, while active probing rates are set individually from the data rate but introduces pricey overhead. D-ORCD approximates the reply to the fixed point equation using a distributed distance vector approach. The generalization towards the systems with inter-funnel interference appear to follow along with directly, where, the cost of the generalization is proven is the centralization from the routing/scheduling globally over the network or perhaps a constant factor performance lack of the distributed variants. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively.

REFERENCES:

[1] AbhijeetBhorkar, Member, IEEE, Mohammad Naghshvar, Member, IEEE, and Tara Javidi, Senior Member, IEEE, “Opportunistic Routing With Congestion Diversity inWireless Ad Hoc Networks”, ieee/acm transactions on networking, vol. 24, no. 2, april 2016.

[2] L. Ying and S. Shakkottai, “On throughput-optimal scheduling with delayed channel state feedback,” presented at the 2008 Information Theory and Applications Workshop, San Diego, CA, USA, Feb. 2008.

[3] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, “A high throughput path metric for multi-hop wireless routing,” in Proc. ACM Mobicom, 2003, pp. 134–146.

[4] P. Gupta and T. Javidi, “Towards throughput and delay optimal routing for wireless ad hoc networks,” in Proc. Asilomar Conf., 2007, pp. 249–254.

[5] S. Sarkar and S. Ray, “Arbitrary throughput versus complexity tradeoffs in wireless networks using graph partitioning,” IEEE Trans. Autom. Contr., vol. 53, no. 10, pp. 2307–2323, Nov. 2008.

[6] E. Leonardi, M. Mellia, M. A. Marsan, and F. Neri, “Optimal scheduling and routing for maximum network throughput,” IEEE/ACM Trans. Netw., vol. 15, no. 6, pp. 1541–1554, Dec. 2007.

[7] A. SHAIKH, A. VARMA, L. KALAMPOUKAS, AND R. DUBE, “ROUTING STABILITY IN CONGESTED

BALANCING TRADE-OFFS IN MERGE ARTICULATED CONDUIT AND REVERSE FORCE NAVIGATION

Dr Janardhan Antharam[1]., A.Shirisha[2]., Bairi Santoshi[3]., G.Shravani[4] ., M Sai Priya[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- dhana48@yahoo.co.in)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0502, 16RG1A0509, 16RG1A0531, 16RG1A0558),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

*Abstract— **In comparison, you are able to that the opportunistic variant of backpressure, diversity backpressure routing ensures bounded expected total backlog for those stabilizable arrival rates. D-ORCD with single destination is demonstrated to make sure a bounded expected delay for those systems and under any admissible traffic, as long as the speed of computations is sufficiently fast in accordance with traffic statistics. Opportunistic routing mitigates the outcome of poor wireless links by exploiting the broadcast nature of wireless transmissions and also the path diversity. E-DIVBAR is suggested: when selecting the following relay one of the groups of potential forwarders, E-DIVBAR views the sum differential backlog and also the expected hop-count towards the destination. The present property of ignoring the price towards the destination, however, becomes the bane of the approach, resulting in poor delay performance in low to moderate traffic. The primary contribution of the paper is to supply a distributed opportunistic routing policy with congestion diversity to which, rather of the simple addition utilized in E-DIVBAR, the congestion details are integrated using the distributed shortest path computations. We reveal that an identical analytic guarantee could be acquired concerning the throughput optimality of D-ORCD. Particularly, we prove the throughput optimality of D-ORCD by searching in the convergence of D-ORCD to some centralized form of the formula.***

Keywords— Stabilizable, congestion measure, Lyapunov analysis, opportunistic routing, queuing stability, routing policy.

1. INTRODUCTION

We think about the problem of routing packets across a multi-hop network composed of multiple causes of traffic and wireless links while making certain bounded expected delay. Each packet transmission could be overheard with a random subset of receiver nodes among that the next relay is chosen opportunistically. When multiple streams of packets will be to traverse the network, however, it may be desirable to route some packets along longer or even pricier pathways, if these pathways eventually result in links which are less congested [1]. More precisely, the opportunistic routing decisions come in a web-based manner by selecting the following relay in line with the actual transmission outcomes in addition to a rank ordering of neighboring nodes. To make sure throughput optimality, backpressure-based algorithms make a move completely different. This very property of ignoring the price towards the destination, however, becomes the bane of the approach, resulting in poor delay performance in low to moderate traffic. E-DIVBAR is suggested: when selecting the following relay one of the groups of potential forwarders, E-DIVBAR views the sum differential backlog and also the expected hop-count towards the destination. The primary contribution of the paper is to supply a distributed opportunistic routing policy with congestion diversity (D-ORCD) to which, rather of the simple addition utilized in E-DIVBAR, the congestion details are integrated using the distributed shortest path computations. We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed QualNet simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality. Within this work, however, we've selected to concentrate our comparative analysis around the following solutions in literature that have similar overhead, complexity, and practical structure: ExOR, DIVBAR, and E-DIVBAR. Under this insurance policy packets are routed based on a rank ordering from the nodes with different congestion measure [2]. In addition, we suggested an operating distributed and asynchronous 802.11 compatible implementation of D-ORCD, whose performance was investigated using a detailed group of QualNet simulations for practical and realistic systems. The primary challenge in the style of minimum-delay routing policies is balancing the trade-off between routing the packets across the shortest pathways towards the destination and disbursing the traffic based on the maximum backpressure. Compared, D-ORCD may very well be a packet-based form of the min-backlogged-path routing without an excuse for the enumeration of pathways over the network and/or pricey computations of total backlog along pathways. In addition, this paper proposes an operating implementation of D-ORCD which empirically optimizes critical formula parameters as well as their effects on delay in addition to protocol overhead. In addition, while LIFO-Backpressure policy guarantees stability with minimal queue-length variations, realistic burst traffic in large multi-hop wireless systems may lead to queue-length variations and unnecessarily high delay.

2. CLASSICAL DESIGN:

The opportunistic routing schemes could possibly cause severe congestion and unbounded delay. In comparison, you are able to that the opportunistic variant of backpressure, diversity backpressure routing ensures bounded expected total backlog for those stabilizable arrival rates. To make sure throughput optimality, backpressure-based algorithms make a move completely different: instead of using any metric of closeness towards the destination, they pick the receiver using the largest positive differential backlog [3]. Disadvantages of existing system: Other existing provably throughput optimal routing policies distribute the traffic in your area inside a manner much like DIVBAR and therefore, lead to large delay. E-DIVBAR doesn't always create a better delay performance than DIVBAR.

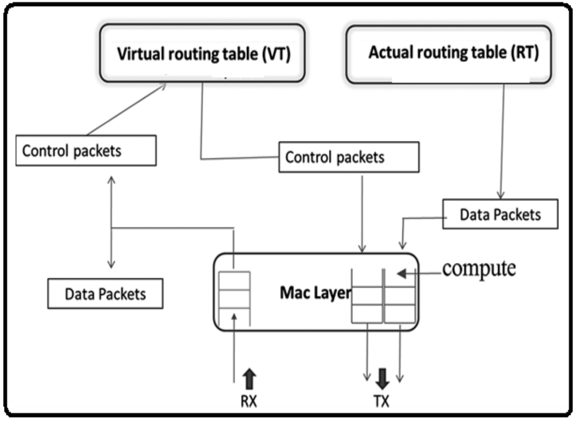


Fig.1.Proposed block diagram

3. ROBUST SCHEME:

An extensive analysis from the performance of D-ORCD is supplied in 2 directions: We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination (single commodity) and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality [4]. Throughout the transmission stage, a node transmits a packet. Within this paper, we provided a distributed opportunistic routing policy with congestion diversity by mixing the key facets of shortest path routing with individuals of backpressure routing. Simulations demonstrated that D-ORCD consistently outperforms existing routing algorithms. Benefits of suggested system: We reveal that D-ORCD exhibits better delay performance than condition-of-the-art routing policies concentrating on the same complexity, namely, ExOR, DIVBAR, and E-DIVBAR. We reveal that the relative performance improvement over existing solutions, generally, depends upon the network topology but is frequently significant used, where perfectly symmetric network deployment and traffic the weather is uncommon. The optimality from the centralized option would be established using a type of Lyapunov functions suggested.

Implementation: Throughout the acknowledgment stage, each node which has effectively received the transmitted packet, transmits an acknowledgment towards the transmitter node. D-ORCD then takes routing decisions with different congestion-aware distance vector metric, known as the congestion measure. D-ORCD uses routing table each and every node to look for the next best hop. The routing table at node includes a listing of neighbors along with a structure composed of believed congestion measure for those neighbors in connected with various destinations. The routing table functions like a storage and decision component in the routing layer. The temporary congestion measures are computed inside a fashion much like a distributed stochastic routing computation of utilizing the backlog information at the outset of the computation cycle. More precisely, node periodically computes its very own congestion measure and subsequently advertises it to the neighbors using control packets at times of seconds. More particularly, throughout the relaying stage, the relaying responsibility from the packet is now use a node using the least congestion measure among those that have obtained the packet. The congestion way of measuring a node connected having a given destination provides approximately the perfect draining duration of a packet coming at this node until it reaches destination. Finally the particular routing table is updated while using records within the virtual routing table after every second [5]. Noting the expected transmission time at node for that packet may then be approximated. We discuss the implementation problems with D-ORCD, especially, distributed and asynchronous iterative Computations. We offer a short discussion from the fundamental challenges of D-ORCD such as the three-way handshake procedure employed in the MAC layer, link quality estimation, avoidance of loops while routing, and overhead reduction issues. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively. One of the leading challenges within the implementation of the opportunistic routing formula, generally, and D-ORCD particularly, is the style of an 802.11 compatible acknowledgement mechanism in the MAC layer. Here we propose an operating and straightforward method to implement acknowledgement architecture. Specifically, before any transmission, transmitter performs funnel sensing and starts transmission following the back off counter is decremented to zero. The priority ordering determines the virtual time slot where the candidate nodes transmit their acknowledgement [6]. Nodes within the set which have effectively received the packet then transmit acknowledgement packets sequentially within the order based on the transmitter node. Within our implementation, we've cheated the priority-based queuing D-ORCD prioritizes the control packets by assigning them the greatest strict priority, lowering the probability the packets are delivered to the MAC layer as well as making certain a prompt receiving the control packets. Furthermore, D-ORCD scheduler assigns a sufficiently lower PHY rate for that control packets. In passive probing, the overhearing capacity from the wireless medium is required. The nodes are configured to promiscuous mode, hence enabling these to hear the packets from neighbors. In passive probing, the MAC layer monitors the amount of packets caused by the neighbors such as the retransmissions. We've extended the rule to D-ORCD by advertising the routes as unreachable to greater rated nodes. Particularly, you can easily observe that this overhead cost, i.e., the entire quantity of ACKs sent per data packet transmission, increases linearly with how big the group of potential forwarders. Thus, we think about a modification of D-ORCD by means of opportunistically routing with partial diversity [7]. We think about the modifications of D-ORCD with partial diversity and choose the amount of neighbors which acknowledge the reception from the packet. This analysis characterizes the trade-off between performance and also the overhead cost connected with receiver diversity. In Split-horizon with poison reverse, a node advertises routes as unreachable towards the node by which these were learned. Without effort, this process penalizes the routes with loops and removes them in the group of available alternatives. Finally, a weighted average can be used to mix the active and passive estimates to look for the link success odds.

3. CONCLUSION:

The aim of this paper would be to design a routing policy with improved delay performance over existing opportunistic routing policies. We advise a period-different distance vector, which helps the network to route packets via a neighbor using the least believed delivery time. D-ORCD opportunistically routes a packet using three stages of: transmission, acknowledgment, and relaying. We provided theoretical throughput optimality evidence of D-ORCD. In D-ORCD, we don't model the interference in the nodes within the network, but rather leave that issue to some classical MAC operation. Passive probing doesn't introduce any extra overhead cost but could be slow, while active probing rates are set individually from the data rate but introduces pricey overhead. D-ORCD approximates the reply to the fixed point equation using a distributed distance vector approach. The generalization towards the systems with inter-funnel interference appear to follow along with directly, where, the cost of the generalization is proven is the centralization from the routing/scheduling globally over the network or perhaps a constant factor performance lack of the distributed variants. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively.

REFERENCES:

[1] AbhijeetBhorkar, Member, IEEE, Mohammad Naghshvar, Member, IEEE, and Tara Javidi, Senior Member, IEEE, “Opportunistic Routing With Congestion Diversity inWireless Ad Hoc Networks”, ieee/acm transactions on networking, vol. 24, no. 2, april 2016.

[2] L. Ying and S. Shakkottai, “On throughput-optimal scheduling with delayed channel state feedback,” presented at the 2008 Information Theory and Applications Workshop, San Diego, CA, USA, Feb. 2008.

[3] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, “A high throughput path metric for multi-hop wireless routing,” in Proc. ACM Mobicom, 2003, pp. 134–146.

[4] P. Gupta and T. Javidi, “Towards throughput and delay optimal routing for wireless ad hoc networks,” in Proc. Asilomar Conf., 2007, pp. 249–254.

[5] S. Sarkar and S. Ray, “Arbitrary throughput versus complexity tradeoffs in wireless networks using graph partitioning,” IEEE Trans. Autom. Contr., vol. 53, no. 10, pp. 2307–2323, Nov. 2008.

[6] E. Leonardi, M. Mellia, M. A. Marsan, and F. Neri, “Optimal scheduling and routing for maximum network throughput,” IEEE/ACM Trans. Netw., vol. 15, no. 6, pp. 1541–1554, Dec. 2007.

A COLLABORATIVE PUBLISHING DEPENDS ON SECRET CODE VALUES

Dr ANBUNATHAN[1]., G.SUDESHNA[2]., NEETHI SHALOM[3]., B. MEGHANA [4] ., JADHAV KAVERI[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- anubunathan.r@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0523, 15RG1A0560, 15RG1A0507, 16RG1A0538),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract*— Differential privacy is an infinitely more rigorous privacy model. It takes the released information is insensitive towards the addition or removal of merely one record. Within this paper, we try to solve this concern and propose a mechanism that may verify if the utility from the printed data is equivalent to the utility claimed through the writer without compromising the information privacy, namely disclosing the raw data, even if your writer is dishonest. Our proposal solves the task to ensure the utility from the printed data in line with the encrypted frequencies from the original data records rather of the plain values. Both DiffPart and DiffGen safeguard data privacy at the fee for data quality. We think about the problem of directly computing the utility of ultimate data printed via differential privacy inside a horizontally distributed context. We concentrate on the classical frequent itemset mining formula Apriori within this paper. The providers then sequentially verify the auxiliary datasets to determine whether their information is properly involved. In some instances, the information publishers might even cheat within this process for a number of reasons. And lastly, anyone can compute a straight line transformation from the utility from the released dataset in ciphertext with individual's verified auxiliary datasets and verify if the utility could be recognized. An easy method to prevent such occasions would be to ask them to write their raw data along with their papers for supervision. we present our experiments to judge the effectiveness and efficiency in our proposal.

***Keywords*— Apriori algorithm, collaborative data publishing, utility verification, differential privacy.**

1. INTRODUCTION

Within this paper, we first propose a privacy-preserving utility verification mechanism based on cryptographic way of DiffPart - a differentially private plan created for set-valued data. Such scenarios, the information users could have a strong demand to determine the utility from the printed data because most anonymization techniques have negative effects on data utility. To apply this model, the related anonymization mechanisms will often have to include noise towards the printed data, or probabilistically generalize the raw data. Within this paper, we classify the information to become printed into two classes: set-valued data and relational data [1] [2]. We first propose a privacy-preserving utility verification mechanism for DiffPart, a differentially private anonymization formula created for set-valued data. Then we extend the above mentioned mechanism to DiffGen, a differentially private anonymization formula created for relational data. Mohammed et al. described differentially private means of releasing horizontally and vertically distributed data. However, lots of differentially private methods happen to be suggested to deal with several types of data. The generalization of the categorical attribute is dependent on a set taxonomy tree. Non-interactive systems publish all of the sanitized data previously so the miners get full accessibility printed data. This provides researchers much greater versatility in performing the needed analysis. As all of the intermediate datasets are encrypted by our probabilistic cryptosystem, it's infeasible for that user or even the providers to understand more information concerning the raw data between any neighboring inputs [3].

2. SYSTEM DESIGN:

Lots of privacy models and corresponding anonymization mechanisms have been proposed within the literature for example k-anonymityanddifferential privacy Kay-anonymity and it is variants l-diversity and t-closeness safeguard privacy by generalizing the records so that they can't be distinguished from another records. Differential privacy Isa a lot more rigorous privacy model. It takes that the released information is insensitive towards the addition or elimination of single record. Disadvantages of existing system: Each one of these data anonymization mechanisms have serious negative effects around the data utility [4]. Consequently, the people that use the printed data will often have a powerful demand to ensure the actual utility from the anonym zed data. This is very challenging because utility computing usually requires to understand the raw data, which, however, ought to be hidden in the verifier because of privacy concerns. In some instances, the information publishers might even cheat within this process for a number of reasons.

3. ANANYMIZATION APPROACH:

We first propose a privacy-preserving utility verification mechanism for DiffPart, a differentially private anonymization formula created for set-valued data. DiffPartperturbs the frequencies from the records with different context-free taxonomy tree with no products within the original data are generalized. Our proposal solves the task to ensure the utility from the printed data in line with the encrypted frequencies from the original data records rather of the plain values. Consequently, it may safeguard the initial data in the verifying parties (i.e., the information users) simply because they cannot learn whether or the number of occasions a particular record seems within the raw dataset not understanding its real frequency [5]. Additionally, because the encrypted frequencies are supplied through the writer, we present a plan for those verifying parties to incrementally verify its correctness. Then we extend the above mentioned mechanism to DiffGen, a differentially private anonymization formula created for relational data. Not the same as DiffPart, DiffGenmay generalize the attribute values before perturbing the regularity of every record. Information losses come from both generalization and also the perturbation. These 2 kinds of information losses are measured individually by distinct utility metrics. We take both into account. Our analysis implies that the utility verification for generalization operations could be transported by helping cover their just the printed data. Consequently, this verification doesn't need any protection. The utility metric for that perturbation is comparable with this for DiffPart. We thus adapt the suggested privacy-preserving mechanism for this verification. We conduct a number of experiments upon the real world set-valued data and relational data to judge the efficiency from the suggested mechanisms. The outcomes reveal that these mechanisms are efficient enough so long as both data publishing and utility verification are offline. Benefits of suggested system: Our theoretical analysis demonstrates the correctness and also the security from the suggested mechanism. We think about the problem of directly computing the utility of ultimate data printed via differential privacy inside a horizontally distributed context.

Fundamental Information: Barthes et al. suggested a framework for reasoning on differential privacy. The partition of DiffPart in every round is dependent on a context free taxonomy tree that ignores the subterranean dataset, and therefore is deterministic. While DiffGen uses an exponential mechanism to pick an applicant for specialization in every round in line with the subterranean dataset, and therefore the partition is probabilistic. we slightly revise this definition to help make the verification require only homomorphic additions [6]. Within the novel plan for utility verification from the dataset printed by DiffPart or DiffGen within this paper, the writer will release several encrypted auxiliary datasets all of which are encrypted with this particular cryptosystem.

Structure Implementation: Within our system, the writer supports the complete raw data To aggregate from distributed data providers. With regards to collaborative data publication, these providers safely upload their raw data to some central writer who's certain to never disclose these data with other parties such as the providers. One fix for your problem is applying a completely distributed privacy preserving CDP plan counting on no central facility. The utility verifiers could be either the people that use the printed data or data providers. Prior to the incremental verification protocol, the writer collects the information posted by all of the providers, performs the differentially private mechanism. For example, like a typical set valued data, market basket information is generally examined for mining frequent itemsets. Therefore, within this paper, we must make use of the central writer and assume it might never reveal any provider's raw data to the 3rd party including other providers. The implementation from the solutions is performed in C programming language. To be able to provide sufficiently strong guarantee of information security, the safety parameter transported within the cryptosystem is placed [7]. The general public key may each provider as the private secret is shared one of the providers with a couple secret discussing techniques guaranteeing that no provider can recover it individually. Then, the precision from the mining results ought to be a much better utility metric within this situation compared to distinction between the printed and also the original data. To write relational data without compromising data privacy, differentially private mechanisms always execute a generalization first and publish the generalized data with their perturbed frequency.

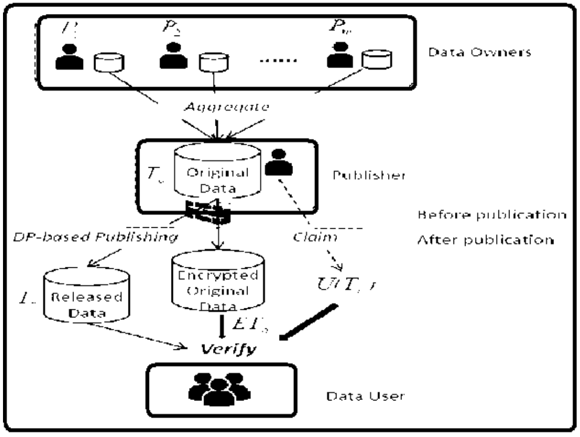


Fig.1.System architecture.

4. CONCLUSION:

Our proposal solves the task to ensure the utility from the printed data in line with the encrypted frequencies from the original data records rather of the plain values. The outcomes reveal that these mechanisms are efficient enough so long as both data publishing and utility verification are offline. Furthermore, it's enabled to independently look into the correctness from the encrypted frequencies supplied by the writer, which will help identify dishonest publishers. We extend this mechanism to DiffGen - another differentially private publishing plan created for relational data. To ensure the utility from the printed data, our proposal requires producing several auxiliary datasets in ciphertext form. DiffPart recursively assigns the records to related nodes of the context-free taxonomy tree and perturbs the frequencies before publishing. The center of every cluster will be accustomed to represent other records within the cluster. The data loss for every printed record is measured through the average relative error from the frequency of every item within the set with regards to the original record.

REFERENCES:

[1] Jingyu Hua, An Tang, Yixin Fang, Zhenyu Shen, and Sheng Zhong, “Privacy-Preserving Utility Verification of the DataPublished by Non-interactive DifferentiallyPrivate Mechanisms”, IEEE Transactions on Information Forensics and Security, 2016.

[2] Shangfu Peng, Yin Yang, Zhenjie Zhang, Marianne Winslett, and Yong Yu. Query optimization for differentially private data management systems. In Proceedings of the 29th International Conference on Data Engineering (ICDE’13), pages 1093–1104, 2013.

[3] Liyue Fan, Li Xiong, and Vaidy Sunderam. FAST: differentially private real-time aggregate monitor with filtering and adaptive sampling. In Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data (SIGMOD’13), pages 1065–1068, 2013.

[4] Rui Chen, Benjamin Fung, Bipin C. Desai, and N´eriah M. Sossou. Differentially private transit data publication: A case study on the montreal transportation system. In Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD’12), pages 213–221, 2012.

[5] Jian Xu, Wei Wang, Jian Pei, Xiaoyuan Wang, Baile Shi, and Ada Wai-Chee Fu. Utility-based anonymization for privacy preservation with less information loss. ACM SIGKDD Explorations Newsletter, 8(2):21–30, 2006.

[6] Nabeel Mohammed, Dima Alhadidi, Benjamin Fung, and Mourad Debbabi. Secure two-party differentially private data release for vertically partitioned data. Dependable and Secure Computing, IEEE Transactions on, 11(1):59–71, 2014.

[7] Elaine Shi, T-H. Hubert Chan, Eleanor G. Rieffel, Richard Chow, and Dawn Song. Privacy-preserving aggregation of time-series data. In Proceedings of the 18th Network and Distributed System Security Symposium (NDSS’11), 2011.

CONFIDENCE BREAKING IN PUBLIC COMMUNICATION USING USER'S WILLINGS

Dr.S.P.Malarvizhi[1]., Byram Kalyani [2]., C.Hari Keerthana[3]., A.Laxmi Prasanna[4] ., K.Varshitha[5]
1 Professor, Department of CSE., Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India (✉:- spmalarvizhi1973@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0511, 16RG1A0512, 16RG1A0504, 16RG1A0549),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

*Abstract***—** ***To higher serve users' various social communication needs, OSNs give a huge assortment of internet features for his or her users to take part in, for example building connections, delivering messages, uploading photos, browsing friends' latest updates, etc. To validate the potency of social behavior profile in discovering account activity anomaly, we use the social behavior profile of every user to distinguish clickstreams of their particular user all other users. We investigate portrayal of person user's social behaviors to identify account usage anomaly. Many activities on OSNs require multiple steps to accomplish. Typical OSNs classify social information into different page types. Time a person requires to complete each action of the given activity is heavily affected by the user's social characteristics. We present the combined measurement outcomes of each behavior feature for those users to exhibit the worth space, and lastly we make use of an example as one example of user behavior diversities. We further process each clickstream before performing detailed measurement analysis. Mix-validation can be used to make certain that every a part of data can be used for both training and validation, and it makes sense not produced from biased data. We conduct three teams of experiments by different training data size, feature quality, and profile completeness, correspondingly, to judge their impacts upon the recognition precision. We adjust the brink of the amount of sample activities to understand more about if the feature vector quality affects the recognition precision. The greater kinds of activities a person conducts, the greater complete its behavior profile could be. A user's record distributions of individuals feature values comprise its behavior profile.***

*Keywords***—** ***Clickstream, online social behavior, privacy, data analysis, compromised accounts detection, cross-validation.***

1. INTRODUCTION

According to our observation of user interaction with various OSN services, we advise several new behavior features that may effectively evaluate user variations in online social activities. A social behavior profile precisely reflects a user's OSN activity patterns. While a genuine owner conforms to the account's social behavior profile involuntarily, it's hard and pricey for impostors to feign. Despite the fact that a user's credential is hacked, a malicious party cannot easily have the user's social tendencies with no charge of the physical machines the clickstreams [1] [2]. Yang et al. investigated connections among identified spammers along with other malicious account recognition methods exploit the variations on static profile or connectivity information between normal and malicious accounts. By recording a user's message posting features, for example timing, topics and correlation with buddies, they detected irregular posting behaviors however, all messages inside a certain duration are clustered in line with the content, and also the clusters by which most messages are published by irregular behaviors are called from compromised accounts. Typical OSNs give a huge assortment of social activities to fulfill their users' communication needs. Throughout a single trip to a website, a person may request multiple information. To be able to observe both extroversive and introversive behaviors in the participating users, we create a browser extension to record user activities on Face book by means of clickstreams [3].

2. TRADITIONAL APPROACH:

Previous research on spamming account recognition mostly cannot distinguish compromised accounts from Sybil accounts, with simply one recent study by Egeleet al. features compromised accounts recognition. Existing approaches involve account profile analysis and message content analysis. However, account profile analysis is hardly relevant for discovering compromised accounts, as their profiles would be the original common users' information which will probably remain intact by spammers [4]. Disadvantages of existing system: Malicious parties exploit the well-established connections and trust relationships between your legitimate account proprietors as well as their buddies, and efficiently distribute junk e-mail ads, phishing links, or adware and spyware, while staying away from being blocked through the providers. Major OSNs today employ IP geolocation logging to fight against account compromisation. However, this method may are afflicted by low recognition granularity and false positive rate. URL blacklisting has got the challenge of timely maintenance increase, and message clustering introduces significant overhead when exposed to a lot of real-time messages.

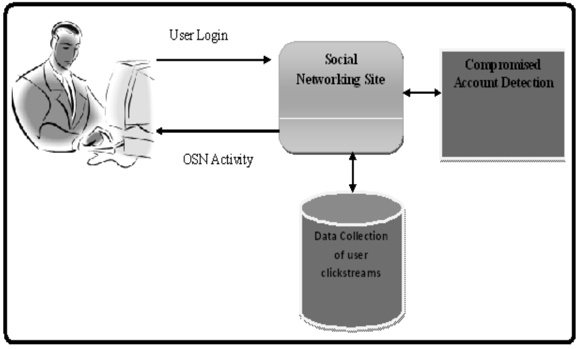

User Login
Social Networking Site
Compromised Account Detection
OSN Activity
Data Collection of user clickstreams

Fig.1.System architecture

3. ENHANCED DESIGN:

Rather of analyzing account contents or message contents, we seek to locate the behavior anomaly of compromised accounts using legitimate owners' history social activity patterns, which may be noticed in a light-weight manner. To higher serve users' various social communication needs, OSNs give a huge assortment of internet features for his or her users to take part in, for example building connections, delivering messages, uploading photos, browsing friends' latest updates, etc. However, the way a user involves in every activity is totally driven by personal interests and social habits. Consequently, the interaction patterns with numerous OSN activities are usually divergent across a sizable group of users. While a person has a tendency to comply with its social patterns, a hacker from the user account you never know little concerning the user's behavior habit will probably diverge in the patterns. Around the corner of the aforementioned intuition and reasoning, we first conduct research on online user social behaviors by collecting and analyzing user clickstreams of a common OSN website. According to our observation of user interaction with various OSN services, we advise several new behavior features that may effectively evaluate user variations in online social activities [5]. For every behavior feature, we deduce a behavior metric by acquiring a record distribution from the value ranges, observed from each user's clickstreams. Furthermore, we combine the particular behavior metrics of every user right into a social behavior profile, addressing a user's social tendencies. Benefits of suggested system: To validate the potency of social behavior profile in discovering account activity anomaly, we use the social behavior profile of every user to distinguish clickstreams of their particular user all other users. We conduct multiple mix-validation experiments, each with different quantity of input data for building social behavior profiles. Our evaluation results reveal that social behavior profile can effectively differentiate individual OSN users with precision as much as 98.6%, and also the more active a person, the greater accurate the recognition.

Social Behaviors: Because of the many activities and WebPages, the potential value spaces of these two features are extremely large. Normal user activities have a tendency to explore merely a small part of these feature value spaces [6]. According to our Face book measurement study, we evaluate Face book user tendencies into some eight fine-grained metrics that match the eight social behavior features. We apply our understanding acquired within the Face book measurement study, and devise a quantification plan for every behavior feature. With concrete behavior metrics in hands, we develop a Face book user's social behavior profile beginning with mixing their social behavior metrics into an 8-vector tuple, then normalizing each vector so the amount of all elements inside a vector equals to 1. Giving fat loss on every feature would be to portray a user's amount of consistency on several behavior features, also is hard to feign. Heavy-weighted behavior features that the user behaves more consistently on play more essential roles in discovering impostors than light-weighted features. First, human behaviors are intrinsically non-deterministic, therefore a tiny bit of variation is anticipated even for the similar activity done by exactly the same user. Second, since the social behavior profile is made on the top of record observations, errors always exists for a finite quantity of samples. Heavy-weighted behavior features that the user behaves more consistently on play more essential roles in discovering impostors than light-weighted features [7]. To capture the modification, working out phase could be repeated utilizing a user's latest clickstream to update a user's behavior profile including feature weights. Hence, a threshold from the minimum quantity of sample activities ought to be assigned to be sure the quality of metric vectors. Our evaluation on sample Face book users signifies that people is capable of high recognition precision when behavior profiles are made inside a complete and accurate fashion.

4. CONCLUSION:

Within this paper, we read the social behaviors of OSN users, i.e., their use of OSN services, and the use of which in discovering the compromised accounts. Major OSNs today employ IP geolocation logging to fight against account compromisation. Offline analyses of tweets and Face book posts demonstrate that most junk e-mail are distributed via compromised accounts, rather of dedicated junk e-mail accounts. The rate of actions whenever a user participates in certain extroversive activities reflects the user's social interaction style. We denote the beginning of a session whenever a user begins to visit Face book in almost any window or tab of the browser the finish of the session is denoted once the user closes all home windows or tabs that visit Face book, or navigates from Face book in most home windows or tabs from the browser. For example, if your user's extroversive activity metric vectors aren't available because of the reason why it doesn't conduct extroversive activities. Additionally, we compare the outcomes between your student users and also the online-employed users. our method could be adopted in conjunction with existing schemes to fight against account hijacking.

REFERENCES:

[1] Xin Ruan, Zhenyu Wu, Member, IEEE, Haining Wang, Senior Member, IEEE, and Sushil Jajodia, Fellow, IEEE, "Profiling Online Social Behaviors for Compromised Account Detection", ieee transactions on information forensics and security, vol. 11, no. 1, january 2016.

[2] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing spammers' social networks for fun and profit: A case study of cyber criminal ecosystem on Twitter," in Proc. 21st Int. Conf. World Wide Web (WWW), Lyon, France, 2012, pp. 71–80.

[3] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user behavior in online social networks," in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), Chicago, IL, USA, 2009, pp. 49–62.

[4] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine learning," in Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), Geneva, Switzerland, 2010, pp. 435–442.

[5] C. Yang, R. C. Harkreader, and G. Gu, "Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers," in Proc. 14th Int. Conf. Recent Adv. Intrusion Detection (RAID), Menlo Park, CA, 2011, pp. 318–337.

[6] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and evaluation of a real-time URL spam filtering service," in Proc. IEEE Symp. Secur. Privacy (S&P), Oakland, CA, USA, May 2011, pp. 447–462.

[7] D. Wang, D. Irani, and C. Pu, "Evolutionary study of Web spam: Webb spam corpus 2011 versus Webb spam corpus 2006," in Proc. IEEE Int. Conf. Collaborative Comput., Netw., Appl. Worksharing (CollaborateCom), 2012, pp. 40–49.

AN INFERENCE SCHEME BASED ON POLITICAL ISSUES AND ELECTORAL INFO

G Naga Kumar Kakarla[1]., J.Pravallika[2]., G.Divyanjali [3]., J.Vaishnavi[4] ., K.Gamya Bai[5]

1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- kumarkgn@yahoo.co.in)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0537, 16RG1A0530, 16RG1A0536, 16RG1A0548),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract— ***A prerequisite for answering the above mentioned research questions is the opportunity to precisely estimate the political leaning of people involved. Given retweet and retweeted information are helpful for inferring a Twitter account's political leaning, we formulate inference like a graph Laplacian-egularized least squares problem featuring its two steps. Prior understanding can readily be integrated into our inference technique as constraints of the optimization problem. Sources transporting a serious leaning, e.g., the election candidates themselves may serve as anchors with fixed political leaning xi. Used, a resource can concurrently be scarcely retweeted and also have low similarity along with other sources. In record inference, solving ill-posed problems requires us to include prior understanding from the problem to eliminate undesirable solutions. we give a regularization term towards the least squares problem to make sure similar Twitter users, i.e., individuals getting similar teams of audience who've retweeted them, have similar political leaning. retweet information is better quality than follower data. Retweeting is frequently an action of approval or recognition, but following continues to be proven to become of the different nature. Because the quantity of data readily available for analysis is restricted because when fast the press sources publish, researchers might need to aggregate data produced over lengthy amounts of time, frequently years, to do reliable analysis. A prerequisite for answering the above mentioned research questions is the opportunity to precisely estimate the political leaning of people involved. The temporal dynamics of political leaning and polarization were also studied. Our optimization framework can readily be adapted to include other kinds of information. Our methodology is relevant with other OSNs with retweet-like endorsement mechanisms, for example Face book and YouTube with "like" functionality.***

Keywords— ***Twitter, political science, data analytics, inference, convex programming, signal processing***

1. INTRODUCTION

Our technique requires only a steady flow of tweets although not the Twitter social networking, and also the computed scores possess a simple interpretation of "averaging," Within this paper, we read the problem of quantifying and inferring the political leaning of Twitter users. The Twitter API prevents crawling the network past the one-hop neighborhood of the couple of 1000 nodes [1]. However, our method requires just one link with the actual-time Twitter stream to gather retweets. Volkova et al. built a number of Twitter social graphs to enhance neighbors' features to enhance performance. We find out the Twitter accounts of two major media sources, one with liberal and yet another with conservative leaning. The act of retweeting carries implicit sentiment from the retweeted. This is correct whether or not the original tweet doesn't carry any sentiment itself. By concentrating on the election candidates4 and official political party accounts, we have seen a obvious separation of these two camps: two same-camp accounts have similarity. The task of solving ill-posed problems is within picking out a reasonable solution from the infinite group of achievable solutions. From the computational perspective it's beneficial to sparsely the matrix, therefore we also evaluate our formula by having an extra k-nearest-neighbor step [2].

2. TRADITIONAL METHOD:

A number of methods happen to be suggested to evaluate the level of bias in traditional press. Indirect methods involve linking media outlets to reference points with known political positions. For instance, Lott and Hassett linked the sentiment of newspaper headlines to economic indicators. Groseclose and Milyo linked media outlets to Congress people by co-citation of think tanks, after which assigned political bias scores to media outlets in line with the Americans for Democratic Action (ADA) lots of Congress people. Gentzkow and Shapiro performed an automatic analysis of text content in newspaper articles, and quantified media slant because the inclination of the newspaper to make use of phrases more generally utilized by Republican or Democrat people from the Congress [3]. Disadvantages of existing system: Poor Twitter, accurate political leaning estimation poses two key challenges: Can you really assign significant statistical scores to tweeters of the position within the political spectrum? Exactly how should we devise a technique that leverages the size of Twitter data while respecting the speed limits enforced through the Twitter API? A far more fundamental issue is data scarcity. Because the quantity of data readily available for analysis is restricted because when fast the press sources publish, researchers might need to aggregate data produced over lengthy amounts of time, frequently years, to do reliable analysis [4]. Analyzing media sources through their OSN outlets offers many unparalleled possibilities rich in volume data from interaction using their audience.

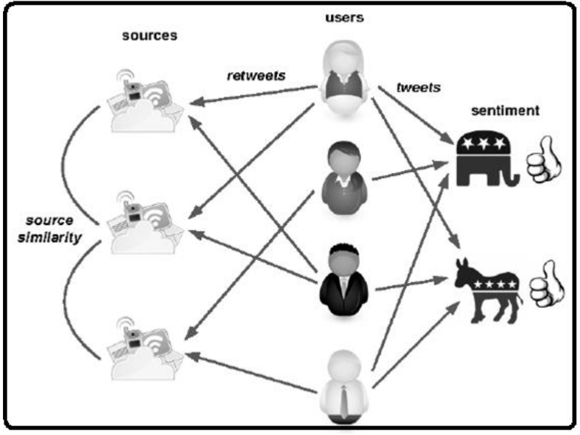


Fig.1.Proposed system framework

3. ADVANCED DESIGN:

Our technical contribution would be to frame political leaning inference like a convex optimization problem that jointly maximizes tweet-retweet agreement by having an error term, and user similarity agreement having a regularization term that is built also to take into account heterogeneity in data. Our technique requires only a steady flow of tweets although not the Twitter social networking, and also the computed scores possess a simple interpretation of "averaging," i.e., a score may be the average quantity of positive/negative tweets expressed when retweeting the prospective user [5]. Liberals dominate the populace of less vocal Twitter users with less retweet activity, however for highly vocal populations, the liberal-conservative split is balanced. Partisanship also increases with localness of people. Hash tag usage patterns change considerably as political occasions unfold. Being an event is going on, the increase of Twitter users taking part in the discussion helps make the active population more liberal and fewer polarized. Benefits of suggested system: It was to outshine many baseline algorithms. Using its reliability validated, we applied it to evaluate some prominent retweet sources, after which propagated their political leaning to some bigger group of ordinary Twitter users and hash tags. Our optimization framework can readily be adapted to include other kinds of information.

Implementation: We defined the dates of the event the following: the beginning date was identified according to our understanding from the event, e.g., the beginning duration of a presidential debate, and also the finish date was understood to be your day when the amount of tweets arrived at a nearby minimum or dropped below those of the beginning date. While there are lots of options to defining and constructing ground truth, our option is motivated by our implicit assumption of Twitter political leaning to be the perceived leaning with a source's retreaters. For every source we compute its feature vector because the term frequencies from the 23,794 hash tags utilized by the very best 1,000 sources [6]. Then we train an SVM classifier while using 900 from the top 1,000 sources that aren't labeled by 12 human idol judges as training data. To help support our claim, we compute the inter-rater agreement in our manual labels as Fleiss' k = .430. We adjusted the provided lexicon by compiling a higher-frequency tweet-word list per event, after which removing words13 that people envisage to not carry sentiment poor elections. We compare the political leaning scores learnt by our technique with "ground truth" built by human evaluation. When it comes to classification, we discover the retweet network based techniques to work most effectively. Particularly, a mix of modularity maximization and label propagation produces precision and recall values near to individuals because of our method. When it comes to classification, we discover the retweet network based techniques to work most effectively. Particularly, a mix of modularity maximization and label propagation produces precision and recall values near to individuals because of our method. Ideas consider a great way to estimate it while using political leaning lots of the very best retweet sources. For every hash tag, we compute its political leaning because the average of sources which have tried on the extender at least one time within their printed tweets [7]. On a single hands, a celebration draws attention from less vocal users who will probably have weak political leaning, and join the discussion because everybody discusses it. However, the truth that a usually silent user joining the discussion may suggest she's strongly opinionated concerning the subject.

4. CONCLUSION:

Our technical contribution would be to frame political leaning inference like a convex optimization problem that jointly maximizes tweet-retweet agreement by having an error term, and user similarity agreement having a regularization term that is built also to take into account heterogeneity in data. Regularization is much more essential for sources with inadequate information available. The prevalent utilization of online social systems (OSNs) to disseminate information and exchange opinions, by everyone, press and political actors alike, has allowed new avenues of research in computational political science. While using learnt political leaning scores, we try to evaluate political polarization of the population, however for this to become possible we first require a polarization measure. Using its reliability validated, we applied it to evaluate some prominent retweet sources, after which propagated their political leaning to some bigger group of ordinary Twitter users and hash tags. Liberals outnumber conservatives in every day, whether or not it's an event day or otherwise. It seems the increase of users throughout an event drives polarization from the Twitter population lower, since these extra users generally have less strong political leaning.

REFERENCES:

[1] Felix Ming Fai Wong, Member, IEEE, Chee Wei Tan, Senior Member, IEEE, Soumya Sen, SeniorMember, IEEE, Mung Chiang, Fellow, IEEE, “Quantifying Political Leaning from Tweets,Retweets, and Retweeters”, IEEETransactions on Knowledge and Data Engineering, 2016.

[2] M. Gentzkow and J. M. Shapiro, “What drives media slant? Evidence from U.S. daily newspapers,” Econometrica, vol. 78, no. 1, pp. 35–71, January 2010.

[3] S. Ansolabehere, R. Lessem, and J. M. Snyder, “The orientation of newspaper endorsements in U.S. elections,” Quarterly Journal of Political Science, vol. 1, no. 4, pp. 393–404, 2006.

[4] S. A. Munson, S. Y. Lee, and P. Resnick, “Encouraging reading of diverse political viewpoints with a browser widget,” in Proc. ICWSM, 2013.

[5] U. N. Raghavan, R. Albert, and S. Kumara, “Near linear time algorithm to detect community structures in largescale networks,” Physical Review E, vol. 76, no. 3, 2007.

[6] J. Wang, W. X. Zhao, Y. He, and X. Li, “Infer user interests via link structure regularization,” ACM Transactions on Intelligent Systems and Technology, vol. 5, no. 2, 2014.

[7] M. Laver, K. Benoit, and J. Garry, “Extracting policy positions from political texts using words as data,” American Political Science Review, vol. 97, no. 2, 2003.

CONTENT-DEPENDENT VISUAL EXTRACTION STRATEGY FOR SIMILARITY SEARCH

Dr.Joseph Prakash Mosiganti[1]., Akanksha Jha[2]., G.P.S Chaitanya Reddy[3]., K.Yamini[4] ., K.Sureshini[5]

1 Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- mjosephp7@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0505, 16RG1A0529, 16RG1A0554, 16RG1A0553),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract*— We present a singular framework of internet Multimodal Distance Metric Learning, which concurrently learns optimal metrics on every individual modality and also the optimal mixture of the metrics from multiple modalities via efficient and scalable online learning this paper investigates a singular framework of internet Multi-modal Distance Metric Learning, which learns distance metrics from multi-modal data or multiple kinds of features with an efficient and scalable online learning plan. OMDML takes benefits of online learning approaches for high quality and scalability towards large-scale learning tasks. Like a classical well-known online learning technique, the Perceptions formula simply updates the model with the addition of an incoming instance having a constant weight whenever it's misclassified. Although various DML algorithms happen to be suggested in literature, most existing DML methods generally fit in with single-modal DML for the reason that they become familiar with a distance metric either on one kind of feature or on the combined feature space simply by concatenating multiple kinds of diverse features together. To help lessen the computational cost, we propose a minimal-rank Online Multi-modal DML formula, which avoids the necessity of doing intensive positive semi-definite projections and therefore saves a lot of computational cost for DML on high-dimensional data.

***Keywords*— OMDML, Content-based image retrieval, multi-modal retrieval, distance metric learning, online learning, low-ranking**

1. INTRODUCTION

Locating a long way metric/function remains a wide open challenge for content-based multimedia retrieval tasks till now. Distance metric learning (DML) is a vital method to improve similarity search in content-based image retrieval. Despite being studied extensively, most existing DML approaches typically adopt just one-modal learning framework that learns the space metric on whether single feature type or perhaps a combined feature space where multiple kinds of features are merely concatenated. We further propose a minimal-rank OMDML formula which by considerably reducing computational costs for top-dimensional data without PSD projection The goal of CBIR would be to search images by analyzing the particular items in the look instead of analyzing metadata like keywords, title and author, so that extensive efforts happen to be accomplished for investigating various low-level feature descriptors for image representation [1]. Existing DML studies could be grouped into different groups based on different learning settings and concepts. the past few years have witnesses an outburst of active research efforts in style of various distance/similarity measures on some low-level features by exploiting machine learning techniques. Such single-modal DML methods are afflicted by some critical limitations: (i) some form of features may considerably dominate others within the DML task because of diverse feature representations and (ii) learning a distance metric around the combined high-dimensional feature space could be very time-consuming while using naive feature concatenation approach. Our jobs are also associated with multimodal/multi view studies that have been broadly studied on image classification and object recognition fields. We present a singular framework of internet Multimodal Distance Metric Learning, which concurrently learns optimal metrics on every individual modality and also the optimal mixture of the metrics from multiple modalities via efficient and scalable online understanding how to address these limitations, within this paper, we investigate a singular plan of internet multi-modal distance metric learning (OMDML), which explores a unified two-level online learning plan: (i) it learns to optimize a distance metric on every individual feature space and (ii) it learns to obtain the optimal mixture of diverse kinds of features. Finally, we observe that our jobs are also not the same as some existing distance education studies that learn nonlinear distance functions using kernel or deep learning methods [2].

2. CLASSICAL APPROACH:

Recently, one promising direction to deal with this concern would be to explore distance metric learning by making use of machine learning strategies to optimize distance metrics from training data or side information, for example historic logs of user relevance feedback in content-based image retrieval systems. The past few years have observed a number of algorithms suggested to enhance Perceptions, which often stick to the principle of maximum margin learning to be able to increase the margin from the classifier. Included in this, probably the most notable approaches may be the group of Passive-Aggressive learning algorithms, which updates the model whenever the classifier fails to make a large margin around the incoming instance [3]. Disadvantages of existing system: Although various DML algorithms happen to be suggested in literature, most existing DML methods generally fit in with single-modal DML for the reason that they become familiar with a distance metric either on one kind of feature or on the combined feature space simply by concatenating multiple kinds of diverse features together. Inside a real-world application, such approaches are affected from some practical limitations: Some kinds of features may considerably dominate others within the DML task, weakening the opportunity to exploit the potential for all features and also the naïve concatenation approach may lead to a combined high dimensional feature space, making the following DML task computationally intensive.

3. ENHANCED OMDML:

This paper investigates a singular framework of internet Multi-modal Distance Metric Learning, which learns distance metrics from multi-modal data or multiple kinds of features with an efficient and scalable online learning plan. The important thing ideas of OMDML are twofold: It learns to optimize another distance metric for everybody modality, also it learns to locate an ideal mixture of diverse distance metrics on multiple modalities. We present a singular framework of internet Multimodal Distance Metric Learning, which concurrently learns optimal metrics on every individual modality and also the optimal mixture of the metrics from multiple modalities via efficient and scalable online learning. We further propose a minimal-rank OMDML formula which by considerably reducing computational costs for top-dimensional data without PSD projection [4]. We provide theoretical research into the OMDML method. We do an extensive group of experiments to judge the performance from the suggested approaches for CBIR tasks using multiple kinds of features. Benefits of suggested system: OMDML takes benefits of online learning approaches for high quality and scalability towards large-scale learning tasks. To help lessen the computational cost, we propose a minimal-rank Online Multi-modal DML formula, which avoids the necessity of doing intensive positive semi-definite projections and therefore saves a lot of computational cost for DML on high-dimensional data. Further, we suggested the reduced-rank online multi-modal DML formula, which not just runs more proficiently and scalable, but additionally achieves the condition-of-the-art performance one of the competing algorithms within our experiments.

Implementation: We make reference to this open research problem like a multi-modal distance metric learning task, and offer two new algorithms to resolve it within this section. When a triplet of images is received, we extract different low-level feature descriptors on multiple modalities from all of these images. Once the training information is abundant and computing sources are comparatively scarce, some existing studies demonstrated that the correctly designed OGD formula can asymptotically approach or perhaps outshine a particular batch learning formula [5]. Besides, we observe that the work was partly inspired through the recent study of internet multiple kernel learning which aims to deal with online classification tasks using multiple kernels. The important thing challenge to online multi-modal distance metric learning tasks would be to develop a competent and scalable learning plan that may optimize both distance metric on every individual modality and meanwhile optimize the combinational weights of various modalities. Clearly this formula naturally preserves the PSD property from the resulting distance metric. We pinpointed some major limitations of traditional DML approaches used, and presented the internet multi-modal DML method which concurrently learns both optimal distance metric on every individual feature space and also the optimal mixture of multiple metrics on various kinds of features.

Analysis of Formula: Generally, it is easy to demonstrate the above mentioned theorem by mixing the outcomes from the Hedge formula and also the PA online learning, like the technique used. We currently evaluate the theoretical performance from the suggested algorithms [6]. To create side information by means of triplet instances for understanding the ranking functions, we sample triplet constraints in the images within the training set based on their ground truth labels. To extensively assess the effectiveness in our algorithms, we compare the suggested two online multi-modal DML algorithms. This paper investigated a singular group of online multimodal distance metric learning algorithms for CBIR tasks by exploiting multiple kinds of features. To help lessen the costly price of DML on high-dimensional feature space, we advise a minimal-rank OMDML formula which not just considerably cuts down on the computational cost but additionally maintains highly competing as well as learning precision. To judge the retrieval performance, we adopt the mean Average Precision and top-K retrieval precision. Like a broadly used IR metric, mAP value averages the typical Precision (AP) value of all of the queries, because both versions denotes the region under precision recall curve for any query [7]. Finally, with regards to the time cost, the suggested LOMDML formula is significantly more effective and scalable compared to other algorithms, which makes it simple for large-scale applications.

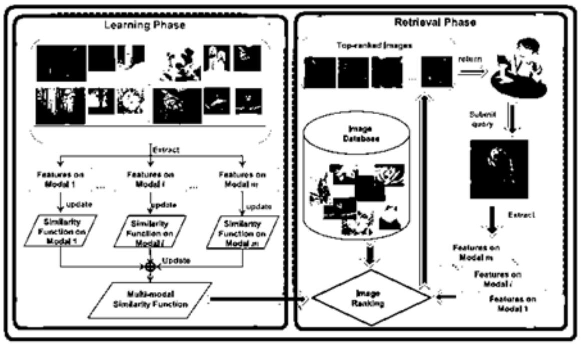


Fig.1.Proposed model

4. CONCLUSION:

This paper investigates a singular framework of internet Multi-modal Distance Metric Learning, which learns distance metrics from multi-modal data or multiple kinds of features with an efficient and scalable online learning plan. When a triplet of images is received, we extract different low-level feature descriptors on multiple modalities from all of these images. The important thing challenge to online multi-modal distance metric learning tasks would be to develop a competent and scalable learning plan that may optimize both distance metric on every individual modality and meanwhile optimize the combinational weights of various modalities. Once the training information is abundant and computing sources are comparatively scarce, some existing studies demonstrated that the correctly designed OGD formula can asymptotically approach or perhaps outshine a particular batch learning formula. OMDML takes benefits of online learning approaches for high quality and scalability towards large-scale learning tasks. We conduct extensive experiments to judge the performance from the suggested algorithms for multi-modal image retrieval, by which encouraging results validate the potency of the suggested technique.

REFERENCES:

[1] Pengcheng Wu, Steven C. H. Hoi, Peilin Zhao, Chunyan Miao, and Zhi-Yong Liu, “Online Multi-Modal Distance Metric Learningwith Application to Image Retrieval”, ieee transactions on knowledge and data engineering, vol. 28, no. 2, february 2016.

[2] W. Di and M. Crawford, “View generation for multiview maximum disagreement based active learning for hyperspectral image classification,” IEEE Trans. Geosci. Remote Sens., vol. 50, no. 5, pp. 1942–1954, May 2012.

[3] D. Wang, S. C. H. Hoi, P. Wu, J. Zhu, Y. He, and C. Miao, “Learning to name faces: A multimodal learning scheme for search-based face annotation,” in Proc. 36th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2013, pp. 443–452.

[4] J. Yang, Y.-G. Jiang, A. G. Hauptmann, and C.-W. Ngo, “Evaluating Bag-of-visual-words representations in scene classification,” in Proc. ACM Int. Conf. Multimedia Inf. Retrieval, 2007, pp. 197–206.

[5] S. C. Hoi, W. Liu, M. R. Lyu, and W.-Y. Ma, “Learning distance metrics with contextual constraints for image retrieval,” in Proc. IEEE Conf. Comput. Vis. Pattern Recog., New York, NY, USA, Jun. 17–22 2006, pp. 2072–2078.

[6] L. Yang, R. Jin, L. B. Mummert, R. Sukthankar, A. Goode, B. Zheng, S. C. H. Hoi, and M. Satyanarayanan, IEEE Trans. Pattern Anal. Mach. Intell., vol. 32, no. 1, pp. 30–44, Jan. 2010.

A COMPLEX NET SHARE SCHEME FOR MULTI-LEVEL HIERARCHY IN OPEN NETS

Sujatha Godavarthi[1]., B.Meghana[2]., A.Amulya Deepthi[3]., G.Sindhu[4] ., G.Amrutha[5]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- sujathamantra@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0507, 16RG1A0503, 16RG1A0524, 16RG1A0526),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract— ***In this article, the cloud-computing proposes a knowledgeable disc hierarchy attribute-based file encryption plan. In order to deal with the topic of many hierarchical directories, we advise on a layered access system. For the FH-club penguin-ABE programmed, we perform and conduct a detailed experiment. The cost and time of file encryption in the existing system are high and the system understanding certain time and computer costs are also high. The layered access systems are incorporated into a single access system and are then encrypted using an optimized access structure. Files can be used to share the text portion of ciphers associated with attributes. Club penguin-ABE feasible schemes that are much more versatile and thus more suitable for general applications. Via the layered access structure sort, several hierarchical files are resolved. Both cipher text saving and the file encryption time are saved in the suggested method. With the number of files the, the advantages of our strategy are increasing. Consequently, all cipher storage of text and file encryption time prices are stored. In addition, the proposed proposal is seen to be safe under the normal assumption***

Keywords— Hierarchical file sharing, cipphertext, encryption, cloud service provider

1. INTRODUCTION

Cloud business (CSP) is the cloud server provider which has various customer facilities. The owner of the data encrypts and uploads the cipher text to the CSP. The interested CSP cipher text is downloaded by the user, and encoded. The popular files also have a hierarchy that is hierarchical. In this analysis, the cloud storage called the hierarchy file Club penguin-ABE strategy proposes a qualified encryption scheme according to the layered form of access structure. The shared documents have the sign of multilevel hierarchy, particularly in healthcare and also the military [1]. However, the hierarchy structure of shared files is not explored in Club penguin-ABE. Cipher text-policy attribute-based file encryption is a preferred file encryption technology to resolve the cruel problem of secure data discussing in cloud-computing. Let's go ahead and take personal health record (PHR). To safely share the PHR information in cloud-computing, someone divides his PHR information M into a double edged sword: private information m1 that could retain the patient’s name, son, phone number, street address, etc.

2. PRELIMINARY SYSTEM:

Sahai and Waters suggested fuzzy Identity-Based File encryption in 2005, that was the prototype of ABE. Latterly, a variant of ABE named Club penguin-ABE was suggested. Since Gentry and Silverberg suggested the very first perception of hierarchical file encryption plan, many hierarchical Club penguin-ABE schemes happen to be suggested. Wan et al. suggested hierarchical ABE plan. Later, Zou gave a hierarchical ABE plan, while the size of secret is straight line using the order from the attribute set [2]. A cipher text policy hierarchical ABE plan with short cipher text can also be studied. During these schemes, parents authorization domain governs its child authorization domains along with a top-level authorization domain creates secret key from the next-level domain. The job of key creation is shipped on multiple authorization domains and also the burden of key authority center is lightened. Disadvantages of existing system: In Existing System cost and time for file encryption is high On any special multiple hierarchical files are utilized and Understanding system some time and computation cost are extremely high.

System Basics: More precisely, access structure, bilinear maps, DBDH assumption, and hierarchical access tree are introduced. User downloads and decrypts the interested cipher text from CSP. The shared files will often have hierarchical structure. That's, several files are split into numerous hierarchy subgroups found at different access levels. When the files within the same hierarchical structure might be encrypted by a built-in access structure, the storage price of cipher text and time price of file encryption might be saved. Authority: It's a completely reliable entity and accepts the consumer enrollment in cloud-computing. Cloud Company: It's a semi-reliable entity in cloud system [4]. Data Owner: its large data must be stored and shared in cloud system. User: It really wants to access a lot of data in cloud system. The procedures of understanding are referred to as below. First of all, the consumer decrypts cipher text and obtains content key by utilizing FH-Club penguin-ABE understanding operation. First of all, authority generates public key and master secret key of FH-Club penguin-ABE plan. Next, authority creates secret key for every user. Thirdly, data owner encrypts content keys underneath the access policy.

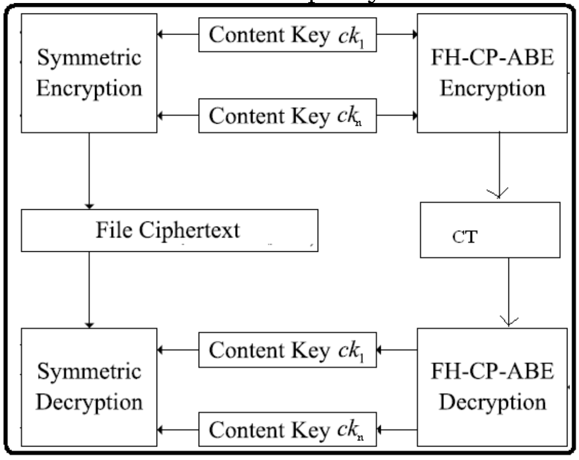


Fig.1.Framework of proposed scheme

3. ENCRYPTION SCHEME:

Within this study, a competent file encryption plan according to layered type of the access structure is suggested in cloud-computing that is named file hierarchy Club penguin-ABE plan. FH-Club penguin-ABE extends typical Club penguin-ABE having a hierarchical structure of access policy, in order to achieve simple, flexible and fine-grained access control. The contributions in our plan are three aspects. First of all, we advise the layered type of access structure to resolve the issue of multiple hierarchical files discussing [4]. The files are encrypted with one integrated access structure. Next, we formally prove the safety of FH-Club penguin-ABE plan that may effectively resist selected plaintext attacks underneath the Decisional Bilinear Diffie-Hellman assumption. Thirdly, we conduct and implement comprehensive experiment for FH-Club penguin-ABE plan, and also the simulation results reveal that FH-Club penguin-ABE has low storage cost and computation complexity when it comes to file encryption and understanding. Benefits of suggested system: The suggested plan comes with an advantage that users can decrypt all authorization files by computing secret key once. Thus, time price of understanding can also be saved when the user must decrypt multiple files. The computation price of understanding may also be reduced if users have to decrypt multiple files simultaneously.

FH-Club penguin-ABE Method: In line with the plan, a better file encryption process about FH-Club penguin-ABE plan is suggested to be able to reduce computational complexity. Additionally, a short discussion FH-Club penguin-ABE Plan With Improved File encryption: In cipher text CT, some transport nodes are taken off CT when they don’t carry any details about level node, in which the information denotes leaf node, non-leaf node, level node, or transport node in hierarchical access tree [5]. Other operations execute just as in Fundamental FH-Club penguin-ABE. Within the phase of Secure of Fundamental FH-Club penguin-ABE, you will find 9 qualified children threshold gates associated with transport nodes in T. the transport node corresponding sub-tree ought to be erased when the transport node isn't level node and every one of the kids nodes from the transport node don’t contain level node, where this is because these transport nodes don't carry any details about level node. Within this paper, we suggested a variant of Club penguin-ABE to efficiently share the hierarchical files in cloud-computing. The hierarchical files are encrypted by having an integrated access structure and also the cipher text components associated with attributes might be shared through the files. Therefore, both cipher text storage and time price of file encryption are saved. When two hierarchy files are shared, the performance of FH-Club penguin-ABE plan is preferable to Club penguin-ABE when it comes to file encryption and decryption’s time cost, and CT’s storage cost. Therefore just the security evidence of FH-Club penguin-ABE ought to be provided. Within this section, the safety bet on the suggested plan is offered first of all. Within the simulation, the FH-Club penguin-ABE scheme’s implementation adopts the raised file encryption formula in file encryption operation [6]. The experimental results reveal that the suggested plan is extremely efficient, particularly when it comes to file encryption and understanding.

4. PREVIOUS STUDY:

Gentry and Silverberg suggested the very first perception of hierarchical file encryption plan, many hierarchical Club penguin-ABE schemes happen to be suggested. The job of key creation is shipped on multiple authorization domains and also the burden of key authority center is lightened. At the moment, you will find three kinds of access structures AND gate, access tree, and straight line secret discussing plan (LSSS) utilized in existing Club penguin-ABE schemes. Eco-friendly et al. and Lai et al. suggested Club penguin-ABE schemes with outsourced understanding to lessen the workload from the understanding user [7]. And Fan et al. suggested a random-condition ABE plan to resolve the issue from the dynamic membership management.

5. CONCLUSION:

In order to enter several hierarchical files, a layered form of access structure is given within the suggested plan. Users will decrypt, when transport nodes are inserted in the access structure with k level nodes, all their authorization files using hidden key calculations. The proposed scheme has the advantage that all authorization files can be decrypted by users once via a hidden computer key. The current proposal has the bonus of users being able to decrypt any consent files once by computing secret key. There when you need to decode several files, time understanding prices can also be saved. The cost of comprehension can also be calculated be saved when the user must decrypt multiple files. The computation price of understanding may also be reduced if users have to decrypt multiple files simultaneously. Furthermore, the suggested plan is demonstrated to become secure under DBDH assumption. Experimental simulation implies that the suggested plan is extremely efficient when it comes to file encryption and understanding.

REFERENCES:

[1] Shulan Wang, Junwei Zhou, Member, IEEE, Joseph K. Liu, Member, IEEE,Jianping Yu, Jianyong Chen, and WeixinXie, “An Efficient File Hierarchy Attribute-BasedEncryption Scheme in Cloud Computing”, ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.

[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated cipher text-policy attribute-based encryption and its application,” in Proc. 10th Int. Workshop Inf. Secur. Appl., Aug. 2009, pp. 309–323.

[3] S. Hohenberger and B. Waters, “Online/offline attribute-based encryption,” in Proc. 17th Int. Conf. Pract. Theory Public-Key Cryptogr. (PKC), vol. 8383. Mar. 2014, pp. 293–310.

[4] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, “Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data,” in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146–166.

[5] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.

[6] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably secure and efficient bounded cipher text policy attribute based encryption,” in Proc. 4th Int. Symp. Inf., Comput., Commun. Secur., Mar. 2009, pp. 343–352.

[7] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, “TIMER: Secure and reliable cloud storage against data re-outsourcing,” in Proc. 10th Int. Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346–358.

RANKING AND EXTRACTING EXACT INFORMATION ON TEXTUAL CONTENT

Suneeta Netala[1]., K.Pallavi [2]., K.Supraja [3]., G.Niharika [4] ., D.Anusha [5]
1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- sunitha_netala@yahoo.co.in)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0542, 16RG1A0550, 16RG1A0532, 16RG1A0515),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— The most important results of a question have probably evolved and come back to be usually the most common framework for XML query processing. We first propose a classy database relaxing architecture to help estimated queries of XML data in order to deal with this problem. These solutions are based on values that can be deduced from the initial query and not specifically comply with the given question formulation. But the existing plans do not take proper account of systems and thus do not have the potential to mix structures with substance in order to address comfortable questions of style. Our solution classifies nodes into two groups: categorical nodes and statistical nodes of attributes and associated approaches to categorical attribute nodes and statistical attribute nodes' similarity relations evaluations. We use a systematic experimental community to demonstrate the power of our proposed approach to accuracy and reminder metrics. In realistic implementations, the querying of XML data also gets intractable as the hierarchical nature of XML documents can be heterogenic and any minor misunderstanding from the database structure will surely raise the possibility of unsatisfactory documentation. Especially when such queries have empty solutions, but no compiler errors, is this very difficult. We also construct a hint based acyclic graph for structure relief and structural organisation, and for this resemblance relationship structural evaluation, we establish an inadequate evaluation coefficient. We therefore develop a new top-quality retrieval method which can intelligently develop the most promising solutions in a ranking-related series.

Keywords— top-k, query relaxations, XML, answer score, querying XML.

1. INTRODUCTION

In functional implementations, the querying of XML data is often unwanted because the hierarchy of XML records can be heterogeneous. A good way to answer an XML request can benefit both the database style query as well as the IR-style query as IRstyle requires an outstanding degree of queried text message to facilitate the query by suggesting a background to perform the search, [1]. A database-style query provides utility for IR-style query. Apart from that, replacements should be presented using the initial query, which you call equivalent substitutes. The estimated queries are feasible In order to help estimated questions about XML data we suggest a query calming process integrating mechanisms and contents and variables that users seem to be more concerned with. Our methodology takes properly into account structures and also the understanding of consumer questions, so that structures and contents can be combated smartly to answer estimated inquiries. These underlying semitone partnerships also have a big impact on the look at the residence and the contents, also it, therefore, is able to stylishly combine structures with contents to reply to approximate queries. Actually, these inherently semantic relationships frequently possess a great affect on the similarity look at the dwelling and also the content. Using the growing recognition of XML for data representations, there's lots of curiosity about searching XML data. Therefore, approximate matching is introduced to handle the difficulty in answering users' queries, which matching might be addressed beginning with relaxing the dwelling and content of the given query and, then, searching for solutions that match the relaxed queries.

Literature Overview: Lately, mixing structured query and text look for answering approximate queries has attracted lots of interest. Maio et al. presented an ontology-based retrieval approach, which assists data organization and visualization and offers an amiable navigation model. In line with the fuzzy tag streams, the issue of purchased tree pattern matching over fuzzy XML data was moved in the next work. We try to improve our query relaxing and ranking method of becomes an update-friendly approach within the dynamic atmosphere [2]. Additionally, we intend to improve our approach, by mixing with emerging semantic technologies, to handle approximate query over structured/unstructured data and linked data. Termehchy and Winslett propose a ranking way of XML keyword search that ranks candidate solutions according to record measures of the cohesiveness. Lately, because of the growing quantity of XML data sources and also the heterogeneous nature of XML data, efficiently evaluating top-k solutions to XML queries continues to be extensively studied.

2. CONVENTIONAL METHOD:

Extensive scientific studies happen to be done on structured queries and also on text search over XML data and graph data. Cellular the problem of formulating the queries with precise structures over XML data, an IR-style querying, particularly, complete-text and keyword search is introduced. This method has got the merit of eliminating structures in the query. It, therefore, lightens you in the burden of understanding the relationships occurring among XML data. Maio et al. presented an ontology-based retrieval approach, which assists data organization and visualization and offers an amiable navigation model. Built around the accessibility to a majority of ontologism, existing commercial solutions accomplish the ontology-based information retrieval and question answering on structured and unstructured data. Fazzinga et al. propose the syntax and semantics of the XPath query language for fuzzy top-k querying in XML. Marian et al. propose an adaptive top-k query-processing strategy in XML that you can use to judge both exact and approximate matches where approximation is determined by relaxing XPath axes. Weigel et al. read the relationship between scoring methods and XML indices for efficient ranking and propose IR-CADG, extra time to data guides to account for keywords, which integrates ranking on structures and contents. Yan et al. propose a desire-based ranking model to cope with approximate queries in XML. Disadvantages of existing system: This method is affected with an inherently limited capacity within the semantics it may express. Additionally, users cannot specify precisely what amount of the database ought to be incorporated within the result because of the lack of structures. Developing ontologism is really a time-consuming task, which frequently needs a precise domain expertise to tackle structural and logical difficulties of concepts in addition to conceivable relationships. This provides us an impetus to the concept that seeks for automatic IR&QA solution built around the environment when ontologism isn't available [3].

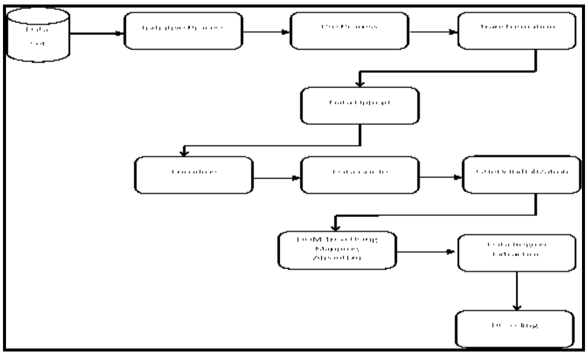


Fig.1.System architecture

3. DESIGNING CURRENT SYSTEM:

We propose sophisticated framework of query relaxations for supporting approximate queries over XML data within this paper. We, then, create a novel top-k retrieval approach that can smartly create the most promising solutions within an order correlated using the ranking measures. Particularly, rather than shifting the responsibility of supplying the similarity functions to the users, our approach can effectively extract the semantics inherently presented within the XML data sources and instantly rank the results satisfying the approximate queries. Benefits of suggested system: We advise a question relaxation method incorporating structures and contents, along with the factors that users are more worried about, for supporting approximate queries overXMLdata. Particularly, our method surmises the factors that users tend to be more worried about based on the analysis of user's original query for supporting query relaxations. Additionally, our approach differentiates the relaxation ordering rather of giving the same importance to each node to become relaxed. Particularly, the very first relaxed structure that need considering is the one which has got the highest similarity coefficient with original query, and also the first node to become relaxed is the most unimportant node. We produce an extensive experimental evaluation, which proves the potency of our proposal on real-world data [4]. We personalize the similarity relation assessment by analyzing the natural semantics presented in XML data sources. In line with the suggested similarity assessment and also the degrees of importance, we complement the query relaxations with a computerized retrieval approach that may efficiently generate probably the most promising top-k solutions.

XML Query Method: Within this paper, we've suggested a classy framework of query relaxations for supporting approximate queries over XML data. We took an information model for XML where details are symbolized as a number of data trees. Basically, an information tree represents part of the real life through entities, values, and relationships included in this. A variety query in XML could be symbolized like a tree pattern query connecting nodes and predicates on values. There are two kinds of edges in E: parent-child edges, written pc, and ancestor-descendant edges. A match of the tree pattern query Q = (LV,E, C) inside a node labeled data tree T describes the solution relation symbolized by Q against data tree T, which is based on single-1 mapping. The semantics of the tree pattern totally taken when it comes to a match.

Approximate Query: Approximately totally done by way of approximately matching strategy, which returns a summary of results according to likely relevance despite the fact that search argument might not exactly match. Query relaxation enables systems to weaken the query constraints to some less restricted form to support users' needs. Generally, query relaxation broadly describes the entire process of altering a question when solutions for this query don't satisfy the user's expectations. Approximate queries could be formally transformed from the given query to a different, and also the transformations included in this can be viewed as from two perspectives: structure relaxation and content relaxation [5]. To prevent generating invalid approximate queries, we can use some structural details about the descendants of distinct nodes in XML documents, which we call a descendant clue. An issue, that's, how you can weaken the restrictions to be able to receive relevant solutions and never weaken an excessive amount of to prevent receiving irrelevant solutions, should be thought about when generating the approximate query. In content relaxations, the scope of the text message is expanded to permit additional solutions to become came back with a query, and also the expanded text message is known as a content substitute. We produce an effective method for searching the very best-k best solutions from a lot of XML data sources together with our query relaxation framework. Finally, the experiments confirm the potency of our suggested approaches. The previous models the similarity relation among confirmed XML tree and it is structural relaxations, grouped using their similarities. The second models the similarity relation of nodes' values, grouped using their similarities. This provides us the muse to exchange an ancestor-descendant edge with two special parent-child edges when assessing the dwelling similarity between your initial query and queries generated by utilizing structural relaxations. While using path similarity coefficient, the similarity of two given pathways might be directly evaluated. Without effort, a tree pattern query includes a number of pathways A node is known as a categorical attribute node if it's a characteristic node and it is connected value is really a categorical value. A node is known as a statistical attribute node if it's a characteristic node and it is connected value is really a statistical value The data in XML data trees could be acknowledged as some real-world entities, because both versions has attributes and interacts along with other entities through relationships symbolized using the connecting pathways [6]. We are saying that two values are connected if their corresponding attribute nodes are interconnections, and 2 ANV pairs are connected if their values are connected. An ANV pair could be visualized like a selection query that binds merely a single attribute node. The Semantic Tree of the given categorical value air connecting by having an attribute node Ai might be built-in two phases. The Semantic Trees contain teams of keywords for every interconnected attribute node within the data trees. Cellular the continuity of statistical values, the purpose introduced, is utilized to estimate the similarity coefficient between two statistical values. With the aid of the lexical database, semantically similar attributes could be identified and processed because the similar attribute throughout the offline step. Identifying the most unimportant attribute node necessitates an ordering of attribute nodes when it comes to their levels worth focusing on.

k-Query Processing and Answer Score: The solution score of the answer measures the relevance of this response to the user's query. For any given parameter k, the very best-k issue is searching the very best top-k solutions purchased from better to the worst. Our content relaxation planning depends on query rewriting. Particularly, the sub threshold for every specified attribute node might be evaluated in line with the corresponding attribute weight [7]. To boost the internet processing efficiency, we're able to recompute the similarity coefficients of categorical attribute nodes and also the standard deviation of statistical attribute nodes, prebaking the approximate values, and make the related indexes throughout the offline processing step. Our approach starts by evaluating all of the structure relaxations and content relaxations, that are maintained using the structure and content relaxation plans ahead of time.

4. CONCLUSION:

Our solution sufficiently takes into consideration the mechanisms and the understanding of users' questions, so it can elegantly merge structures with content in order to answer estimated queries. The solutions behind our proposed system are not obliged to exclusively comply with the given formulation, but may be based on attributes that cannot be deduced from the original inquiry. In contrast, the assistant from segmenting trees and both the categorical or mathematical similarity coefficients are used in accordance with the study into natural semantics shown in XML data sources. In general, our solution applies an equal value to all the attribute nodes for supportive query relaxing, and seems to be more concerned with the user's investigation into the initial query. Our method also takes proper account of structures, so it can elegantly merge structures with contents in order to answer estimated requests. We are now pursuing several fascinating research avenues. Our approach to representative queries with representative database architectures and contents has been tested.

REFERENCES:

[1] Jian Liu and D. L. Yan, “Answering Approximate Queries Over XML Data”, ieee transactions on fuzzy systems, vol. 24, no. 2, april 2016.

[2] H. Mousavi and C. Zaniolo, “Fast and accurate computation of equi-depth histograms over data streams,” in Proc. Int. Conf. Extending Database Technol., 2011, pp. 69–80.

[3] S. Amer-Yahia, N. Koudas, A. Marian, D. Srivastava, and D. Toman, “Structure and Content Scoring for XML,” in Proc. Int. Conf. Very Large Data Bases, 2005, pp. 361–372.

[4] J. Lu, T. W. Ling, C. Chan, and T. Chen, “From region encoding to extended dewey: On efficient processing of XML twig pattern matching,” in Proc. Int. Conf. Very Large Data Bases, 2005, pp. 193–204.

[5] B. Fazzinga, S. Flesca, and A. Pugliiese, “Top-k answers to fuzzy XPath queries,” in Proc. Int. Conf. Database Expert Syst. Appl., 2009, pp. 822–829.

[6] F. Weigel, H. Meuss, K. U. Schulz, and F. Bry, “Content and structure in indexing and ranking XML,” in Proc. Int. Workshop Web Databases, 2004, pp. 67–72.

[7] A. Termehchy and M. Winslett, “Using structural information in XML keyword search effectively,” ACM Trans. Database Syst., vol. 36, no. 1, pp. 1–45, 2011.

AN IMPORTANT ASPECTS DIGGING WITHOUT REDUNDANCY AND BEST FACTS

Sheetal Kulkarni[1]., K.Shravani [2]., G.Shruthi [3] ., B.Kaveri Eranna[4]., K.Bindu Sri [5]

1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- sheetalkulkarni.925@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0540, 16RG1A0533, 16RG1A0556, 16RG1A0551),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— **We advise to add regular lists to my question faces in the top search engine results and apply the QD Miner process. More specifically, QD Miner collects free text lists, HTML tags and repeated regions into the top search engine pages, classifies them into clusters according to products they include, then grades the clusters and products according to the best results obtained from the lists and products. Our method is general and does not rely on some kind of interpretation of the domain. The main goal of mining varies from the recommended query. Our structured approach, defined as QD Miner, is to immediately delete and group regular lists of free text, HTML tags, and repeated regions in the top search engine results. We further analyze the problem of list replication by modeling fine-grained correlations between lists and penalizing duplicate lists to discover more productive queries. Experimental findings show that QD Miner has several lists and useful question facets. Our solution suggested is general and does not rely on the interpretation of any particular domain. This allows open-domain requests to be managed. Want dependent. Dependent. We remove facets for each question in the top papers, rather than the preset schema for your concerns.**

Keywords: Mining facet, Query facet, faceted search, re-ranking system.

1. INTRODUCTION:

We realize that valuable question knowledge is frequently provided in list formats and repeatedly between the best papers. This is how we encourage you to add regular lists to my question facets and apply a system inside the top search engine pages. By choosing facet items, users may explain their particular function. Then findings of the search engine could be restricted to records that are very important to the items. A question might have multiple facets that summarize the data concerning the query from various perspectives [1]. In order to avoid shown the web pages that are almost duplicated in querys at the very top, we can ranking search engine results again. The query facets are also hierarchical and can be used in addition to standard site search in different areas, including semant search or entity search. Any website material will first be repressed on other websites so that the same lists of contents can appear on separate websites on various occasions. We struggle with the problem of identifying facets of query, which involve many types of phrases or terms that signify and summarise the details found in a question[2]. We think that the key facets of a question are often presented and repeated within the query's top retrieved documents in design for lists, and query facets could be found out by aggregating these significant lists. As a result it can cope with open-domain queries. We discover that quality of query facets is impacted by the standard and the amount of search engine results.

Literature Overview: The graphical model learns how likely an applicant term will be a facet item and just how likely two terms should be manufactured inside a facet. Query reformulation is the procedure of modifying a question that may better match a user's information need, and query recommendation techniques generate alternative queries semantically like the original query. Existing summarization algorithms has sorted out into different groups when it comes to their summary construction methods, kinds of information within the summary, and also the relationship between summary and query. Mining query facets relates to entity search for some queries, facet products are types of entities or attributes [3]. Some existing entity search approaches also exploited understanding from structure of WebPages. A strong overview of faceted search is past the scope of the paper. Most existing faceted search and facets generation systems are made on the specific domain or predefined facet groups.

2. QUERY FACETS:

Finding query facets differs from entity search within the following aspects. First, finding query facets is relevant for those queries, instead of just entity related queries. Second, they have a tendency to come back different types of results. Query facets provide intriguing and helpful knowledge about a question and therefore may be used to improve search experiences in many different ways. First, we are able to display query facets together using the original search engine results within an appropriate way. Thus, users can understand some main reasons oaf query without browsing many pages. Some existing entity search approaches also exploited understanding from structure ofwebpages. Caused by a business search are entities, their attributes, and connected homepages, whereas query facets consist of multiple lists of products, that are not necessarily entities. Disadvantages of existing system: Most existing summarization systems dedicate themselves to generating summaries using sentences obtained from documents. Most existing faceted search and facets generation systems are built on the specific domain or predefined facet groups.

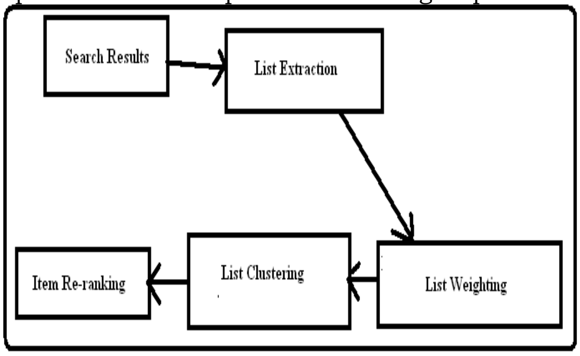


Fig.1.Proposed system architecture

3. ENHANCED SIMILARITY SCHEME:

We advise two models, the initial Website Model and also the Context Similarity Model, to position query facets. Within the Unique Website Model, we think that lists in the same website might contain duplicated information, whereas different websites are independent and every can lead a separated election for weighting facets. We propose the Context Similarity Model, by which we model the fine-grained similarity in between each set of lists. More particularly, we estimate the quality of duplication between two lists according to their contexts and penalize facets containing lists rich in duplication [3]. Within this paper, we explore to instantly find query dependent facets for open-domain queries with different general Web internet search engine. Areas of a question are instantly found in the top web search engine results from the query with no additional domain understanding needed. As query facets are great summaries of the query and therefore are potentially helpful for users to know the query which help them explore information, they're possible data sources which allow a general open-domain faceted exploratory search. Benefits of suggested system: When compared with previous creates building facet hierarchies, our approach is exclusive in two aspects: Open domain. we don't restrict queries in specific domain, like products, people, etc. We discover that quality of query facets is impacted by the standard and the amount of search results. Using more results can generate better facets at the beginning, whereas the advance of utilizing more results ranked less than 50 becomes subtle. We discover the Context Similarity Model outperforms the initial Website Model, meaning we're able to further improve quality. Consequently, different queries may have different facets. Experimental results reveal that quality of query facets mined by QDMiner is nice.

Digging Facets: We implement a method known as QDMiner which finds out query facets by aggregating frequent lists inside the top results. Given a question q, we retrieve the very best K is a result of a internet search engine and fetch all documents to create a set R as input. Then, query facets are found [4]. We define that the container node of the list may be the cheapest common ancestor from the nodes that contains the products within the list. List context is going to be employed for calculating the quality of duplication between lists. Then we employ the pattern item, to extract matched products from each sentence. The very first areas of wrinkles are extracted like a list. It extracts lists from continuous lines that consist of a double edged sword separated with a dash or perhaps a colon. We'll explore these topics to refine facets later on. We'll also investigate other related topics to locating query facets. Good descriptions of query facets might be useful for users to higher comprehend the facets. Instantly generate significant descriptions is definitely an interesting research subject. We named these simple HTML tag based patterns as HTMLTAG. We extract three lists out of this region: a summary of restaurant names, a summary of location descriptions, and a summary of ratings, so we ignore images within this paper. We reason that these kinds of lists are useless for locating facets. We ought to punish these lists, and depend more about better lists to create good facets. Within this paper, the load of the cluster is computed in line with the quantity of websites that its lists are extracted. An easy way of dividing the lists into different groups is examining the websites they fit in with. We think that different websites are independent, and every distinct website has only one separated election for weighting the facet. We discover that the good list is generally based on some and appearance in lots of documents, partly or exactly. For any list obtained from a repeat region, we decide the cheapest common ancestor component of all blocks from the repeat region like a container node. A person list usually contains a small amount of products of the facet and therefore it's not even close to complete The QT formula assumes that information is essential, and also the cluster which has probably the most quantity of points is chosen in every iteration [5]. QT ensures quality by finding large clusters whose diameters don't exceed a person-defined diameter threshold. We assumed that lists from the same website might contain duplicated information, whereas different websites are independent and every can lead a separated election for weighting facets. Because of the existences of the aforementioned cases, there might be duplicated content regions found in different WebPages from various websites, plus they finally generate duplicated lists. Sometimes, two WebPages might just possess a small region that contains duplicated content, however their full content aren't similar enough to become recognized as duplicates by Smash or Shingling. This has the ability to extract all lists as well as their contexts found in all documents, and building their fingerprints into index with less space cost searching engines. During query time, we are able to efficiently calculate similarities between lists after initial facets are generated. Like a better item is generally rated greater by its creator than the usual worse item within the original list.

Implementation Strategy: Within this paper, we read the problem to find query facets. We advise an organized solution, which we describe as QDMiner, to instantly mine query facets by aggregating frequent lists for free text, HTML tags, and repeat regions within top search engine results. For every query, we first ask a topic to by hand create facets and add products that are handled by the query, according to his/her understanding following a deep survey on any related sources [6]. The primary reason for creating this “misc” facet would be to help subjects to differentiate between bad and nudged products. During evaluation, “misc” facets are discarded before mapping generated facets to by hand labeled facets. Clearly we try to rank good facets before bad facets when multiple facets are located. Once we have multi-level ratings, we adopt the neck measure that is broadly utilized in information retrieval, to judge the ranking of query facets. We further make use of the evaluation metrics PRF and wPRF suggested by Kong and Allan. To higher understand the caliber of the generated facets, we show some statistics concerning the generated query facets with clustering parameters. We use fp-nDCG for tuning instead of rp-nDCG because we believe that ranking quality and precision of facets is a lot more important than item recall used. We discover our generated top facets are usually significant and helpful for users to know queries. we use three various kinds of patterns to extract lists from WebPages, namely free text patterns, HTML tag patterns, and repeat region patterns [7]. The repeat region based and HTML tag based query facets have better clustering quality but worse ranking quality compared to free text based ones. The caliber of query facets considerably drops when IDF sits dormant, which signifies the average invert document frequency of products is a vital factor. We discover that Random generates significantly less facets than Top and Top Shuffle. Consequently, the generated facets are often less highly relevant to the query, and in addition they contain less qualified products. We further test out grouping the lists by thinking about the duplication between full-page content, i.e., we make use of the Smash of entire pages that contains lists to calculate list similarities.

4. CONCLUSION:

One list of columns or rows is extracted. We are mainly removing m ·n lists from every table containing m rows and n posts. Each column has: Each block contains a record of the restaurant and contains four characteristics: photograph, name of the restaurant, place description and ranking. In order to assess the calibre of question factors, we construct two human annotated data sets and add current measures and 2 additional combined metrics. Experimental findings show that the method finds useful question facets. We further assess the problem of duplicate lists and find, by assessing their similarities, that facets could be strengthened by modelling thin-grained similarities between lists within a factor between lists inside a facet by evaluating their similarities. The addition of these lists will increase both accuracy and question facet retraction. Part-of-talk data should be used to further investigate lists' homogeneity and increase the caliber of question facets. As nominee subtopics, we have presented question facets within the IMine task of NTCIR-11. Since QD Miner can be enhanced in several ways in the first approach to locating question faces. In order to retrieve further lists in the top scores, for example, several half-checked bootstrapping list extract algorithms can be employs. The retrieval of highly quality lists from authoritative websites can also be rendered by specialized website wrappers.

REFERENCES:

[1] Zhicheng Dou, Member, IEEE, Zhengbao Jiang, Sha Hu, Ji-Rong Wen, and Ruihua Song, “Automatically Mining Facets for Queriesfrom Their Search Results”, ieee transactions on knowledge and data engineering, vol. 28, no. 2, february 2016.

[2] A. Herdagdelen, M. Ciaramita, D. Mahler, M. Holmqvist, K. Hall, S. Riezler, and E. Alfonseca, “Generalized syntactic and semantic models of query reformulation,” in Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. retrieval, 2010, pp. 283–290.

[3] I. Szpektor, A. Gionis, and Y. Maarek, “Improving recommendation for long-tail queries via templates,” in Proc. 20th Int. Conf. World Wide Web, 2011, pp. 47–56.

A DISTINCTIVE STREAMING DESIGN TO FORMALIZING ITS SEMANTIC PRECAUTIONS

Prasanth Kumar Kunda[1]., K.Shravya [2]., G.Rasagna[3] ., D.Niharika [4]., Kaitha Nikhitha[5]

1 Associate Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- kundaas@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (15RG1A0546, 15RG1A0522, 15RG1A0518, 15RG1A0544),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— The CIBPRE method initializes CIBPRE's computer parameters and creates private key systems for users in the stable Key Generation Core. A sender will encrypt the files using the file identity and the file conversation conditions to securely share files to multiple receivers. If the sender wants to speak about a few files linked to similar conditions and others, the sender can delegate to the proxy a re-file cryption key labeled in the proxy condition and in addition to the original receivers of those files also the parameters to produce the re-file encryption confidentiality. For versatile implementations, conditional PRE dependent on identification and PRE broadcasting are appropriate. CIBPRE helps a sender by defining the identity of these recipients to secure a Note for several recipients, and the sender can even delegate to a proxy a re-file encryption substitute for the first cypher document. This paper offers a flexible, primitive programmed called PRE, built on conditional identity and officially offers its semantic security through CPRE, IPRE and BPRE. Furthermore it may also be possible to bind the re-file encryption key to a requirement for re-encoding only matching cypher texts, so that the original sender can implement a thinly-grained access control to his remote cypher texts. Finally, in our CIBPRE we view a credit card programmed that secures the cloud email framework that benefits from the current protected Email networks using the Very Strong Privacy protocol or file encryption based on identity.

***Keywords*— Proxy re-encryption, cloud storage, identity-based encryption, broadcast encryption, secure cloud email**

1. INTRODUCTION

PRE's security traditional ensures that the server/proxy and non-intended recipients cannot learn valuable information about the (re-)encrypted file or that the proxy cannot re-set the first code text in a meaningful way before finding the re-file encryption key. An individual can protect his file with his own public key and then hold ciphertext in a truthful, but uncanny server. The sender will assign a re-file encryption key associated with the recipient to the server through the proxy after a decision is taken by the recipient. In the standard public-clé infrastructure setting, the first PRE was proposed, which involves complicated certificate administration. Just one recipient is allowed by PRE and IPRE[1]. The computer must call PRE or IPRE on several times if there are more recipients. The concept of broadcasting PRE remains proposed in order to address this issue. Even all original cypher texts may be re-secured by the proxy or not. The gross control of the re-encryption of cypher texts can restrict the use of PRE systems. The proxy carrying the corresponding re-scan key will encrypt only the cypher texts fulfilling the requisite requirement. This coarse-acquired control of cipher texts to become re-encrypted may limit the use of PRE systems. To fill this gap, a refined concept known as conditional PRE (CPRE) continues to be suggested. In CPRE schemes, a sender can enforce fine-grained re-file encryption control of his initial cipher texts. The sender achieves this goal by connecting an ailment having a re-file encryption key. Within this paper, we refine PRE by the benefits of IPRE, CPRE and BPRE for additional flexible applications and propose a brand new idea of conditional identity based broadcast PRE. Inside a CIBPRE system, a reliable key generation center initializes the machine parameters of CIBPRE, and generates private keys for users. To safely share files to multiple receivers, a sender can secure the files using the receivers' identities and file-discussing conditions. If later the sender would like to talk about some files connected with similar condition along with other receivers, the sender can delegate a re-file encryption key labeled using the condition towards the proxy, and also the parameters to create the re-file encryption secret is in addition to the original receivers of those files. Then your proxy can re-secure the first cipher texts matching the problem towards the resulting receiver set. Observe that the first cipher texts might be stored remotely and keep secret. The sender doesn't need to download and re-secure repetitively, but delegates just one key matching condition towards the proxy. We define an operating security notion for CIBPRE systems. Without effort, with no corresponding private keys, learn nothing concerning the plaintext hidden within the initial or re-encrypted CIBPRE cipher text a preliminary cipher text cannot be properly re-encrypted with a re-file encryption key when the cipher text and also the key are connected with various conditions. We advise a competent CIBPRE that's provably secure within the above foe model. We prove the IND-sIDCPA security from the suggested CIBPRE plan when the underlying identity-based broadcast file encryption plan is safe and also the Decisional Bilinear Diffie-Hellman assumption holds [2]. Our suggested CIBPRE plan enjoys constant-size initial and re-encrypted cipher texts, and eliminates the restrictions from the recent work. Cloud email product is an encouraging and important application because of its beneficial features. We build an encrypted cloud email system with CIBPRE. It enables a person to transmit an encrypted email to multiple receivers, store his encrypted emails within an email server, review his history encrypted emails, forward his history encrypted emails from the expected susceptible to multiple new receivers. CIBPRE is extremely appropriate for building encrypted cloud email systems and our suggested CIBPRE plan is much more convenient than PGP and IBE to help keep the safety of cloud email system.

2. PREVIOUS MODEL:

PRE and IPRE enables just one receiver. Should there be more receivers, the machine must invoke PRE or IPRE multiple occasions. To deal with this problem, the idea of broadcast PRE continues to be suggested. BPRE works similarly as PRE and IPRE but handier. In comparison, BPRE enables a sender to create a preliminary cipher text to some receiver set, rather of merely one receiver. Further, the sender can delegate a re-file encryption key connected with another receiver set so the proxy can re-secure to. A current conditional proxy broadcast re-file encryption plan enables the senders to manage time to reencrypt their initial cipher texts. Whenever a sender generates a re-file encryption answer to re-secure a preliminary cipher text, the sender needs to accept original receivers' identities from the initial cipher text as input. Used, this means the sender must in your area recall the receivers' identities of initial cipher texts. This requirement makes this plan restricted for that memory-limited or mobile senders and efficient just for special applications. Disadvantages of existing system: The first PRE was suggested within the traditional public-key infrastructure setting which incurs complicated certificate management. The PRE schemes only allow data discussing inside a coarse-grained manner. That's, when the user delegates a reencryption answer to the proxy, all cipher texts could be reencrypt after which be around towards the intended users else no cipher texts could be re-encrypted or utilized by others. PGP and IBE, product is less capable within the facet of communication and never better in consumer experience. Users aren't able to share the encrypted data to other people large amount of issue are occurring. No Identity deliver to public secrets of secure data.

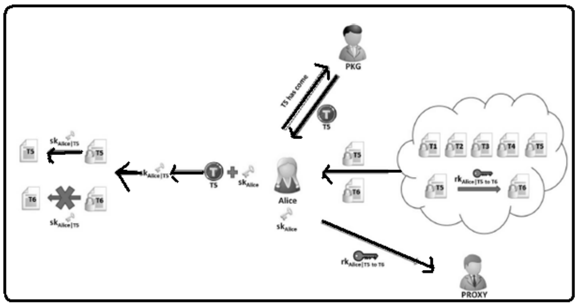


Fig.1.Framework of proposed system

3. PROPOSED SYSTEM:

We advise a competent CIBPRE plan with provable security. Within the instantiated plan, the first cipher text, the re-encrypted cipher text and also the re-file encryption key are in constant size, and also the parameters to develop a re-file encryption key are in addition to the original receivers associated with a initial cipher text. Lately, numerous extended Proxy Re-Encryptions, e.g. Within this paper, we refine PRE by the benefits of IPRE, CPRE and BPRE for additional flexible applications and propose a brand new idea of conditional identity based broadcast PRE. Then your proxy can re-secure the first cipher texts matching the problem towards the resulting receiver set. With CIBPRE, additionally towards the initial approved receivers who can access the file by decrypting the first cipher text using their private keys, the recently approved receivers may also connect to the file by decrypting the re-encrypted cipher text using their private keys. Benefits of suggested system: The sender doesn't need to download and re-secure repetitively, but delegates just one key matching condition towards the proxy. These functions make CIBPRE a flexible tool to secure remotely stored files, particularly when there are various receivers to talk about the files after a while [3]. We define an operating security notion for CIBPRE systems. Without effort, with no corresponding private keys, learn nothing concerning the plaintext hidden within the initial or re-encrypted CIBPRE cipher text a preliminary cipher text cannot be properly re-encrypted with a re-file encryption key when the cipher text and also the key are connected with various conditions. We advise a competent CIBPRE that's provably secure within the above foe model. We prove the IND-sIDCPA security from the suggested CIBPRE plan when the underlying identity-based broadcast file encryption (IBBE) plan is safe and also the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds. Our suggested CIBPRE plan enjoys constant-size initial and re-encrypted cipher texts, and eliminates the restrictions from the recent work.

4. IMPLEMENTATION:

Talking about the idea of CIBPRE, roughly speaking, both initial CIBPRE cipher text and also the re-encrypted CIBPRE cipher text would be the IBBE cipher texts. But it's different by having an IBBE plan that CIBPRE provides algorithms to change an IBBE cipher text into another IBBE cipher text. Furthermore, the transformation is true whether it satisfies the consistencies based on CIBPRE [4]. Therefore, to be able to create a CIBPRE plan, we refers back to the D07 plan that was reviewed. In contrast to the D07 plan, the suggested CIBPRE plan associates a D07 IBBE cipher text with a brand new part to create a preliminary CIBPRE cipher text. This latest part will be employed to realize the capacity ”Conditional” of CIBPRE. Additionally, it offers newer and more effective algorithms, that are correspondingly to develop a reencryption key, re-secure a preliminary CIBPRE cipher text and decrypt a re-encrypted CIBPRE cipher text. The understanding of the initial CIBPRE cipher text is identical using the D07 plan. the IND-Sidcpa security from the suggested CIBPRE plan will disappear towards the DBDH assumption and also the IND-sID-CPA security from the D07 plan [5]. The CIBPRE-based cloud email system includes a reliable KGC (built by a company administrator), a cloud server and users. You can observe that CIBPRE is much more convenient than TRCPBRE used, because the CIBPRE doesn't take extra burden on storage and communication as TR-CPBRE does. Hence it takes extra storage for every sender using the original receivers' identities of generated initial cipher texts, and elevated communication overhead for that proxy to transmit the related S to any or all new receivers of the re-encrypted cipher text. Conclusively, CIBPRE avoids these constraints and helps make the application better. Finally, we coded our CIBPRE plan and tested time price of algorithms [6].

5. CONCLUSION:

The security value of CIBPRE IND-SID-CPA represents CPRE, IPRE and BPRE's protection criteria. For implementations, CIBPRE inherits the advantages of CPRE, IPRE and BPRE. It helps a person to communicate with other individuals in a fine way about their outsourced encrypted data. This paper introduced a brand new PRE term called CIBPRE as well as its IND-sID-CPA safety concepts. This is known as CIBPRE. In reality, the CIBPRE is a general definition built on the capacities of conditional PRE, PRE based on identity and PRE broadcast. The names of all CIBPRE consumers are public secrets of protected records. It prevents an individual from obtaining and verifying certificates from other users before encryption. It also helps an individual to create a broadcast encoder for several receivers and to batch the outsourced encoded data to several recipients. In line with Identity-based Broadcast File Encryption, we instantiated the very first CIBPRE programme. We built the encrypted cloud email system based our CIBPRE plan. In contrast to the prior techniques for example PGP and IBE, In terms of connectivity, our CIBPRE-based method is much more effective and much more practical in customer experience. The demonstration of the CIBPRE is shown to be safe under the IBBE plan and the DBDH assumption under the RO model. It means that, unless a certain key or the authority to exchange outsourced user data is appropriate, little is learned about the user's data. Finally, we compared the proposed strategy of CIBPRE, which focuses on similar work and reinforces the advantages of our plan for CIBPRE.

REFERENCES:

[1] Peng Xu, Member, IEEE, Tengfei Jiao, Qianhong Wu, Member, IEEE,Wei Wang, Member, IEEE, and Hai Jin, Senior Member, IEEE, “Conditional Identity-Based Broadcast ProxyRe-Encryption and Its Application to Cloud Email”, ieee transactions on computers, vol. 65, no. 1, january 2016.

[2] D. Boneh and X. Boyen, “Efficient selective-id secure identitybased encryption without

random oracles," in Proc. Adv. Cryptol., 2004, pp. 223–238.

[3] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., 2009, pp. 279–294.

[4] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., 2011, pp. 1–5.

[5] Q. Tang, "Type-based proxy re-encryption and its construction," in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008, pp. 130–144.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Security, vol. 9, pp. 1–30, 2006

INTEGRATING FAVORABLE OPERABILITY IN OCCURRENCE ASSIST STAND-IN SERVERS

Aluri Brahmareddy[1]., G.Vinitha Sai [2]., D.Sai Sowmya[3] ., H.Shireesha[4]., K.Nandhini [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- brahmareddy475@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (15RG1A0527, 15RG1A0513, 15RG1A0534, 15RG1A0541),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— ***The searchable encryption file (SE) plan is a technology that blends security protection with strong organizational functions which could play an important part in the e-health recording system. A digital medical record product is a unique application that can make healthcare incredibly easy. In this post, we present a special primitive cryptographer called conjunctive keyword search with a tester and a proxy re-encoding feature that is a form of SE-dependent plan. We develop a unique searchable encryption file plan which supports safe conjunctive keyword searches and an accepted delegation feature. Unlike the current arrangements, the job will timely re-file proxy encryption with successful reversal of delegation. The protection and safety of confidential private information will be the most critical issues of users, which could impede further advancement and widespread device adoption. In order to show that the method model is a qualified plan that is stable within its standard model, a Security Model for the proposed Re-dtPECK plan is formulated. The compare and detailed simulations demonstrate a low calculation and overhead storage. It can allow patients to assign partial legal access to search functions to others within a short space of time. The size of the time frame to review and decode the encoded records of the delegator may be tracked.***

Keywords— ***Searchable encryption, time control, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.***

1. INTRODUCTION

Multitudes of realistic, patient-centered electronic health information systems such as Microsoft Health Vault and Google Health have been introduced. Data obtained from the health inside a data centre may contain sensitive data which could potentially lead to the leakage and exposure of persons or businesses who could benefit from the shop. The overarching barrier to large-scale device adoption[1] will be the extreme safety and privacy issues. PRE approach will match the criteria for the proxy re-file encryption. The server will translate the encoded patient index into a re encrypted shape that can be viewed by the delegate. One possible way of solving this problem will be to re-secure all the data with a brand-new key which would cost a lot more. The delegation of a scalable scale would probably be harder to repeal. We attempt to resolve the problem by proposing a new process to automatically revoke the delegation after any time previously specified by the data holders. The information owner is competent to preset diverse effective access periods of time for various users as he appoints his delegation right. A highly effective period of time set through the data owner could be expressed having a beginning and shutting time. Through the re-file encryption formula performed through the proxy server, the timeframe T is going to be baked into the re-encrypted cipher text. It's the timing enabled proxy re-file encryption function. A conjunctive keyword search plan with designated tester and timing enabled proxy reencryption function is suggested. We design a singular searchable file encryption plan supporting secure conjunctive keyword search and approved delegation function. The suggested plan is formally demonstrated secure against selected-keyword selected-time attack. Owner-enforced delegation timing preset is enabled.

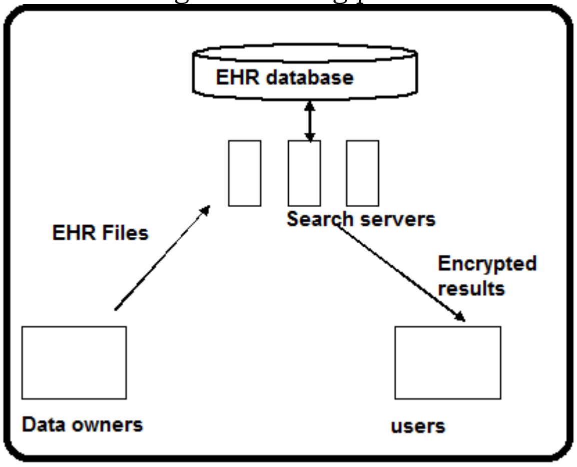


Fig.1.System overview

2. CONVENTIONAL MODEL:

Proxy re-file encryption enables a proxy having a re-file encryption answer to convert a cipher text encrypted with a delegator's public key into individuals that may be decrypted by delegate's private key. Proxy re-file encryption with public keyword search features the idea of keyword search into PRE. You having a keyword trapdoor can search the cipher text as the hidden keywords are unknown towards the proxy. Later, Wang et al. has recommended a better plan to aid the conjunctive keyword search function. Each one of these Re-PEKS schemes are demonstrated secure in random oracle model. Nonetheless, that the proof in random oracle model may most likely produce insecure schemes. Disadvantages of existing system: Existing systems have high communication or computation cost. However, existing schemes require a catalog listing of the queried keywords whenever a trapdoor is generated, that will leak information and impair the query privacy. If the foe finds the trapdoors or encrypted indexes have lower entropies, the KG attacks might be launched when the foe endeavors to guess the potential candidate keywords.

3. PROPOSED SYSTEM:

Within this paper, we try to solve the issue having a novel mechanism suggested to instantly revoke the delegation immediately after some time designated through the data owner formerly. It indicates that users including data owner are restricted when period. The good thing about the suggested product is that there's virtually no time limitation for that data owner since the time details are baked into the re-file encryption phase. The information owner is competent to preset diverse effective access periods of time for various users as he appoints his delegation right. A highly effective period of time set through the data owner could be expressed having a beginning and shutting time. Once the delegate issues a question request, he should produce a trapdoor for that queried keywords using his private key and time seal ST. Only when the timeframe encapsulated within the trapdoor matches using the effective period of time baked into the proxy re-encrypted cipher text, the cloud company will react to looking query. Otherwise, looking request is going to be rejected. By doing so, the access right from the delegate will expire instantly. The information owner needs to avoid every other operation for that delegation revocation. Benefits of suggested system: To the very best of our understanding, this is actually the first work that allows automatic delegation revoking according to timing inside a searchable file encryption system. A conjunctive keyword search plan with designated tester and timing enabled proxy reencryption function is suggested, that has the next merits. Owner-enforced delegation timing preset is enabled. Distinct access period of time could be predefined for various delegate. The suggested plan is formally demonstrated secure against selected-keyword selected-time attack. In addition, offline keyword guessing attacks could be opposed too. The exam formula couldn't function without data server's private key. Eavesdroppers couldn't flourish in guessing keywords through the test formula. The safety from the plan works in line with the standard model instead of random oracle model. This is actually the first primitive that supports above functions and it is built-in the conventional model.

Enhanced Framework: We formally define the conjunctive keyword search having a designated tester and also the timing enabled proxy re-file encryption function. Then, we describe a concrete Re-dtPECK plan having a detailed workflow and derive the correctness from the plan. The Re-dtPECK plan includes following algorithms by having an indicator ?.When its value is 1, the delegation function is going to be activated. Otherwise, the proxy re-file encryption won't be enabled.

Re-dtPEC: Within the system, the Electronic health record documents of the sufferers are encrypted with a symmetric file encryption formula and also the symmetric secret is encapsulated using the patient's public key pkA through the key encapsulation mechanism. The algorithms concentrate on the searchable keywords file encryption and also the timing controlled delegation function [2]. The delegator Ri transmits out a delegation notice towards the reliable 3rd party, time server, proxy server, data server and delegate Rj. The signature could be verified using the public key of Ri . The delegation request might be rejected when the signature is forged. The authority delegation is recognized largely by proxy re-file encryption mechanism. The proxy server take advantage of the re-file encryption answer to transform the cipher text encrypted by delegator's public key into another form, which may be looked through the delegate using their own private key. To have time controlled access right revocation, the predefined time details are baked into the re-encrypted cipher text having a time seal. With the aid of time seal, the delegate has the capacity to produce a valid delegation trapdoor by TrapdoorR formula. When the time information hidden within the re-encrypted cipher text is sporadic with this within the delegation trapdoor, the equation in Test formula won't hold. The individual them self won't be restricted through the effective period of time since the limitation is created within the delegation phase as opposed to the original file encryption phase.

Framework of Re-dtPECK: You will find six entities to have fun playing the interactive process together with a reliable 3rd party (TTP). For example, the Veterans Health Administration (VHA) is assumed to operate like a TTP, who's reliable by clinics, hospitals, patients and doctors [3]. A delegator should be Joe, who's a chronic heart failure patient. The Electronic health record files of Joe are stored on the data server within the cloud inside a protected form. Joe visited Hospital A for that cardiac treatment since February. first, 2014. He wants to designate the cardiologist Dr. Donne from Hospital A to become his delegate for convenient Electronic health record data access. Since Joe intends to transfer to Hospital B after June first and that he hopes that Dr. Donne can't inquiry his Electronic health record that point on. Then, Dr. Donne is granted a period-restricted authority to gain access to the protected health information (PHI) from the patient Joe. Time server (TS) will produce a time seal for Dr. Donne to make sure that they can use of Joe's PHI throughout February. first- May, 30st, 2014. The proxy server (PS) is accountable to secure Joe's PHI to some re-encrypted form to ensure that Dr. Donne can explore individual's records together with his own private key. In phase 1, the TTP initializes the machine by executing Global Setup formula and generates the worldwide parameters. In phase 2, Electronic health record files are created during Joe's therapeutic process. The encrypted Electronic health record indices and documents is going to be generated while using dPECK formula and stored in the cloud data server. Within this system, the signature formula won't be specified. But there's essential around the formula the signature plan ought to be strongly unforgeable. The notice is going to be rejected when the signature fails the verification. If it's verified true, the TTP runs ReKeyGen formula to develop a re-file encryption key and send it towards the PS secretly. The TS runs Time Seal formula to develop a time seal for delegate. When Joe's PHI information is utilized through the Dr. Donne, the PS will run Re-dtPECK formula to encapsulate the effective period of time into re-encrypted cipher text. When the moment isn't in compliance using the effective period of time, the PS won't perform the re-file encryption operation for Dr. Donne. When the delegation indicator ? equals to at least one, phase 3 is going to be performed. Joe transmits a delegation notice towards the TTP, PS, TS, delegate and knowledge server plus a signature signed by Joe. The effective delegation duration of PHI access delegation for delegate is specified. After finding the query, cloud server runs the delegation test formula [4]. The TS runs Time Seal formula to develop a time seal for delegate. When Joe's PHI information is utilized through the Dr. Donne, the PS will run Re-dtPECK formula to encapsulate the effective period of time into re-encrypted cipher text. With this plan, the details are protected using a strong file encryption primitive. The indexes from the conjunctive keywords are encrypted through the dPECK or Re-dtPECK algorithms before submitted towards the cloud server. The company couldn't recover the plaintext from the encrypted data. The keyword extraction from Electronic health record is controlled through the patient and encrypted in your area with patient Ri 's own secret key. However, the outdoors attacker couldn't decide concerning the cipher text of certain keywords and time with no server's private key despite the fact that all of the trapdoors for that other keywords and occasions can be found. IND-KGA guarantees the attackers such as the server attackers and outdoors attackers couldn't discover the relationship between your given trapdoor and also the challenge keywords despite the fact that other trapdoors for delegator and delegate could be acquired. This is because the exam formula could be run when the keyword trapdoor and cipher text are acquired. In PEKS schemes without designated tester, the exam formula could be operated by any attacker. Within this work, the exam formula are only able to be performed through the data server using his private key, the solid concept of "designated tester". The suggested Re-dtPECK is going to be in contrast to other relevant schemes based on these indicators [5]. A simulation result with an experimental test-bed can also be presented to appraise the performance of Re-dtPECK plan. Thus, the suggested plan has various helpful functions and it has more powerful security functionality than individuals of the majority of the existing searchable file encryption schemes. We've evaluated the suggested [6] Re-dtPECK plan by applying critical factors with an experimental work bench, such as the system global setup, the important thing generation, the re-file encryption key generation, the trapdoor generation and also the test algorithms.

4. CONCLUSION:

The trial findings and safety review prove our strategy is much better than current technologies with acceptable cloud overhead. In fact, this is currently the first searchable file encryption plan that uses the proxy re-file encryption timing enabled feature, and the designated HER cloud records privacy-conserving tester. In the course of this article, we proposed a unique Re-DtPECK proposal for the understanding of the scheduling of an electronic healthcare records cloud storage system to protect privacy and enable the automated cancellation of delegations. The connectivity and overhead computing of the proposed options has also been proved by our findings of the simulation for nearly all real-life scenarios. The performance review means that our suggested plan is able to deliver high calculation and storage efficiency, apart from greater security, in contrary to other conventionally searchable file encryption schemes. In addition, after a given period, the delegate can instantly miss the access and control authority. It can also search for conjunctive keywords and avoid attacks by a keyword. By means of the solution, only the tester can verify the existence of such keywords.

REFERENCES:

[1] Yang and Maode Ma, Senior Member, IEEE, “Conjunctive Keyword Search With DesignatedTester and Timing Enabled Proxy Re-EncryptionFunction for E-Health Clouds”, ieee transactions on information forensics and security, vol. 11, no. 4, april 2016.

[2] L. Guo and W. C. Yau, “Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage,” J. Med. Syst., vol. 39, no. 2, pp. 1–11, 2015.

[3] L. Fang, W. Susilo, C. Ge, and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

[4] J. W. Byun and D. H. Lee, “On a security model of conjunctive keyword search over encrypted relational database,” J. Syst. Softw., vol. 84, no. 8, pp. 1364–1372, 2011.

[5] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[6] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ro¸su, and M. Steiner, “Highly-scalable searchable symmetric encryption with support for Boolean queries,” in Advances in Cryptology, Berlin, Germany: Springer, 2013, pp. 353–373.

[7] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, “Further observation on proxy re-encryption with keyword search,” J. Syst. Softw., vol. 85, no. 3, pp. 643–654, 2012.

Face and Expression Recognition through LDN Pattern

Veernala Sireesha[1]., P.Meghana[2]., R Alekhya[3] ., U.Monika[4]., G Akhila [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- veernalasireesha@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0577, 16RG1A0583, 16RG1A0599, 17RG5A0501),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— A binary classifier is trained with manually labeled positive and poor user ratings in the supervised binary emotion classification. We recommend an unlabelled method of classification of mixed-domain sentiment using spectral integrations where all terms and documents are projected to the same lower-dimensional integration. We model the problem as an embedded learning and construct three objective functions to capture: the distributional qualities of the pivots, the mark constraints in the source domain documents and the geometric qualities of both source and target documents in the unlabeled documents. Unlike proposals previous to the source domain feeling labels, which first become acquainted with a smaller embedding and then a feeling classifier within this insert, our popular optimization approach learning embedded products that respond to feeling classification. The supply of the tiny labeled data for this target domain to the labeled information for this source domain and the unlabeled data for the source and target domains is supposed in the supervised adaptation of the domain. However, the supply of labeled data for that target domain is not supposed to take place without supervision domain adaptation. The best result is achieved for one of the individual goals. The inability to recognize an unfavorable feeling of a commodity could lead to lower sales. Our experimental findings on the multi-domain feel classification benchmark data collection indicate that we collectively refine the three objectives often have greater classification accuracy than when we have independently improved each goal. Here, neighboring documents belong to related documents as far as their contents are concerned.

Keywords— Cross-domain, optimization, unsupervised domain, binary classifier

1. INTRODUCTION

Thinking about different classifications of applicable sentiment such as opinion mining, opinion synthesis, contextual advertisements and consumer research, it is not shocking that classification of emotions has gained constant focus. When you think about the variety of goods available online, both are costly as well as unfailing for manual annotation ratings for any kind of product [1]. However, it is enticing to somehow adapt a sentiment classifier learned to characterize the feeling with labeled ratings for a single product. Without monitoring Mix Domain Sentiment Classification may be the job of customized to a new domain (target domain) for a sentiment classifier that has learned in this area, without the need for labeling for this target domain. With a new sentiment classification adapted to previously unseen target areas, we will clear the expense of manually annotated data for that target domain. Our classification domain is known as the root, while the domain we use is known as the prospective. We are familiar with the domination we use. In addition, the proposed approach records mixed domain classification accuracies that are statistically equal to the current state-of-the-art embedding classification system for mixed-domain feelings. One very common way of fixing the classification of mixed-domain feelings will first be to project the root and the objective features into the same lower-dimensional integration and then become aware of an emotion classifier about this built-in space [2].

2. EXISTING SYSTEM:

A very common means to fix mix-domain sentiment classification would be to first project the origin and also the target features in to the same lower-dimensional embedding, and subsequently become familiar with a sentiment classifier about this embedded feature space. This method is especially attractive when there's little overlap between your original source and also the target feature spaces. Similarly distributed words within the source and also the target domains get mapped to closer points within the embedded space, therefore lowering the mismatch of features within the two domains. Prior focus on mix-domains sentiment classification use unlabeled data in the source and also the target domains to first become familiar with a low-dimensional embedding for that two domains. Next, labeled reviews within the source domain are forecasted onto this embedding [3]. Finally, a binary sentiment classifier is trained while using forecasted source domain labeled training instances. Disadvantages of existing system: A limitation of existing two-step approach that decouples the embedding learning and sentiment classifier training would be that the embeddings learnt in the initial step is agnostic towards the sentiment from the documents, the ultimate goal in mix-domain sentiment classification. This process doesn't consider source domain labeled data throughout the PLSR step, making the projection agnostic to sentiment classification. Supervised dimensionality reduction methods are vulnerable to over fitting when the amount of labeled instances are small.

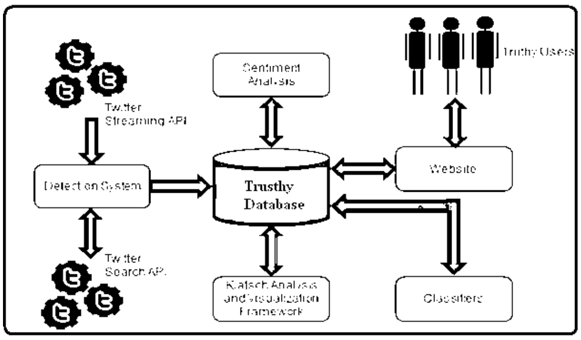


Fig.1.Framework of proposed system

3. CROSS-DOMAIN DESIGN:

We advise an unlabeled mix-domain sentiment classification method using spectral embeddings where we project both words and also the documents in to the same lower dimensional embedding. The embedding learnt by our method enforces three important needs. First, some domain independent features are selected in the source and target domains which should be mapped as near as you possibly can within the embedded space [4]. Second, friend closeness and enemy dispersion from the source domain labeled documents should be preserved. Quite simply, positively labeled documents should be embedded nearer to one another and in the negatively labeled documents. Likewise, negatively labeled documents should be embedded nearer to one another and in the positively labeled documents. Third, within each domain, the neighborhood geometry one of the documents should be preserved. Here, neighbor documents make reference to similar documents when it comes to their text content. We model each one of the above-pointed out needs being an objective function, and jointly optimize the 3 objective functions. Benefits of suggested system: Our experimental results on the benchmark dataset formulation domain sentiment classification show by jointly optimizing the 3 objectives oftentimes we have better classification accuracies than when we had enhanced each objective individually. This result shows the significance of learning embeddings which are responsive to the ultimate task at hands that is sentiment classification. Furthermore, the suggested method considerably outperforms several baselines and formerly suggested embedding learning methods when put on mix-domain sentiment classification.

Sentiment Classification: The distributions of words within the source domain aren't the same as those of the prospective domain. Facets of books like the plot, length, type of writing etc. aren't the same as those of knives like the weight, durability, sharpness, etc. Unigram and bigram lexical-features are obtained from the chosen training instances as features to coach a binary logistic regression classifier with l2 regularization [5]. Even in instances where joint optimization doesn't improve within the individually trained objectives, the performance acquired through the joint optimization technique is never below that acquired through the best individually trained methods. Finally, the load vector learnt through the classifier is recognized as the predictor for w. This will make the job of domain adaptation a frightening one just because a sentiment classifier trained around the source domain reviews will probably perform poorly around the target domain since the features it's learnt in the source domain may not come in the prospective domain. Spectral clustering is conducted about this bipartite graph to produce a lower dimensional representation by which co-occurring domain specific and domain independent features are symbolized through the same group of lower dimensional features. Supervised dimensionality reduction methods like the Fischer Discriminate Analysis views the within and mix-class scattering of information points, when designing lower-dimensional embeddings [6]. Our suggested embedding learning technique is in addition to the pivot selection step so we think that M pivots obtain. The rest of the test is non-pivot ones, which only appear within the two domains. Inside the same domain, we assume the documents are built following a same word distributions, thus, non-pivot words and also the pivots are symbolized through the same unigram and bigram features. The primary technique of mapping the language and documents towards the space would be to first compute the term embeddings, after which derive the document embeddings in line with the word embeddings by thinking about the term occurrences. Although a document is symbolized while using words that come in that document, we can select any feature representation for that individual words. We considered three constraints that must definitely be satisfied by an embedding you can use to coach a mix-domain sentiment classification method. Usually, when multi-dimensional embeddings are computed, you should ensure independence between different embedding dimensions to increase the data provided by the multi-dimensional space and also to avoid redundancy between dimensions [7]. We think about the unweighted mixtures of the various objective functions. We make use of the mix-domain sentiment classification dataset. This dataset includes Amazon . com product critiques for four different product types: books, DVDs, electronics and appliances. We read the relationship between your dimensionality from the embeddings we learn while using suggested method and also the precision acquired around the target domain.

4. CONCLUSION:

The distributions of pivots under the various demands and the manner in which the term distribution influences the distribution of documents between the two domains helps you analyze connections between your documents in both domains. The proposed approach may be applied simply to more than two types of emotions. In comparison to the previously proposed incorporation approaches for the classification of sentimental mixed domain, our approach uses mark knowledge readily accessible for the original domain reviews, which ensures that embedded systems are suited to the ultimate role of implementation, which is the classification of sentiments. In addition to their combinations, we analyzed the efficiency of baby constraints by the use of a benchmark dataset. Our experimental findings demonstrate that some of the variations of the proposed constraints yield results that are statistically similar to the existing state of the art methods for the mixed-domain sensation classification.

REFERENCES:

[1] DanushkaBollegala, Member, IEEE, Tingting Mu, Member, IEEE, andJohn YannisGoulermas, Senior Member, IEEE, “Cross-Domain Sentiment Classification UsingSentiment Sensitive Embeddings”, ieee transactions on knowledge and data engineering, vol. 28, no. 2, february 2016.

[2] J. Blitzer, R. McDonald, and F. Pereira, “Domain adaptation with structural correspondence learning,” in Proc. Conf. Methods Natural Language Process., 2006, pp. 120–128.

[3] E. Kokiopoulou and Y. Saad, “Orthogonal neighborhood preserving projections: A projection-based dimensionality reduction technique,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 12, pp. 2143–2156, Dec. 2007.

[4] D. Bollegala, D. Weir, and J. Carroll, “Using multiple sources to construct a sentiment sensitive thesaurus for cross-domain sentiment classification,” in Proc. 49th Annu. Meet. Assoc. Comput. Linguistics: Human Language Technol., 2011, pp. 132–141.

[5] T. Mu, J. Jiang, Y. Wang, and J. Y. Goulermas, “Adaptive data embedding framework for multi-class classification,” IEEE Trans. Neural Netw. Learn. Syst., vol. 23, no. 8, pp. 1291–1303, Aug. 2012.

[6] N. Halko, P. G. Martinsson, and J. A. Tropp, “Finding structure with randomness: Probabilistic algorithms for constructing approximate matrix decompositions,” SIAM Rev, vol. 53, no. 2, pp. 217–288, 2010.

[7] T. Mu, J. Y. Goulermas, J. Tsujii, and S. Ananiadou, “Proximitybased frameworks for generating embeddings from multi-output data,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 11, pp. 2216–2232, Nov. 2012.

STRUCTURING A HEALTHY AND SAFE MACHINE LEARNING TECHNIQUE

Pedasanaganti Swetha Nagasri[1]., Reddy Likitha [2]., S.Likhitha [3] ., M.Amrutha [4]., P.Bhansri [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- pswetha369@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0585, 16RG1A0588, 16RG1A0563, 16RG1A0581),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— Our suggested semantically improved Marginalized Stacked Denoising Auto encoder can effectively and efficiently learn robust features from the BoW representation. In this important field of study, robust statistical representation learning of texts is a major concern. In this paper we advise you on a brand new approach to representation learning. A semantitic extension from the common deep-learning Denoising Auto-Encoder is developed by our system called Semantical-Enhanced Marginalized Denoising Auto Encode (smSDA). Several research fields are closely connected with the recognition of cyber bullying, including topic recognition and affective analytical analysis. Their activities have allowed them to instantly recognise cyber bullying. Our proposed approach helps us to use the secret framework of bullying knowledge and to uncover a dominant and biassed text representation. Comprehensive tests are being carried out in two public cyber bullying companies and the findings show that our proposed techniques overlap most basic methods of learning to represent the text. The semanticized extension involves semianticized drop-out rumor and sparse limitations on domain-based and embedded approaches to use semantitic drop-out noises. In our suggested model, comprehensive studies on actual data sets have confirmed the results.

Keywords— Marginalized Stacked Denoising Auto encoder, BoW, cyber bullying, fixed-length vectors, latent semantic analysis.

1. INTRODUCTION

Cyber bullying may be defined to be acts of violence by an individual or others, such as transmission of messages and posting comments toward goals, via digital communications techniques. Cyber bullying has become a major issue for teenagers, young people and teens as an unintended result of more and more mainstream social networking. Automatic identification of bullying messages in social networking can be achieved by machine learning strategies that can help build inclusive and secure social networking environments [1]. One of the approaches to addressing the problem of cyber bullying is to recognise and monitor bullying tweets immediately so that appropriate action can be taken to deter future tragedy. Cyber bullying has recently become an important issue for children and young adults, with the increasing recognition of social networking. Previous cyber bullying experiments have focused on comprehensive research and mentally impacting victims, undertaken primarily by social scientists and psychologists. Another favourite text representation model is Latent Semantic Analysis (LSA) and the subject models which correspond with the BoW models. The studied representation can be further processed for different language processing tasks by translating text units into fixed-length vectors. Any ways to address these complaints are proposed from an expert's interpretation of feature learning.

Previous study: The Bag-of-words (BoW) model is easily the most classical text representation and also the cornerstone of some states-of-arts models including Latent Semantic Analysis (LSA) and subject models. The shared deficiency of these aforementioned approaches is built text features continue to be from BoW representation, that has been belittled because of its natural over-sparsity and failure to capture semantic structure [2]. The fundamental idea behind subject models is the fact that word choice inside a document is going to be affected by the subject from the document probabilistically. Subject models attempt to define the generation procedure for each word happened inside a document. Because of their efforts, automatic cyber bullying recognition has become possible. In machine learning-based cyber bullying recognition, there's two issues: 1) text representation understanding how to transform each publish/message right into a statistical vector and a pair of) classifier training. Xu et.al presented several off-the-shelf NLP solutions.

2. PREVIOUS MODEL:

Previous creates computational studies of bullying have proven that natural language processing and machine learning are effective tools to review bullying. Cyber bullying recognition could be formulated like a supervised learning problem. A classifier is first trained on the cyber bullying corpus labeled by humans, and also the learned classifier will be accustomed to recognize a bullying message. Yin et.al suggested to mix BoW features, sentiment features and contextual features to coach an assistance vector machine for online harassment recognition. Dinakaret.al utilized label specific features to increase the overall features, in which the label specific features are learned by Straight line Discriminative Analysis. Additionally, commonsense understanding seemed to be applied. Nahar et.al presented a weighted TF-IDF plan via scaling bullying-like features with a factor of two [3]. Besides content-based information, Maral et.al suggested to use users' information, for example gender and history messages, and context information as additional features. Disadvantages of existing system: The foremost and also critical step may be the statistical representation learning for texts. Next, cyber bullying is difficult to explain and select from the third view because of its intrinsic ambiguities. Thirdly, because of protection of Online users and privacy issues, merely a small part of messages remain on the web, and many bullying posts are deleted.

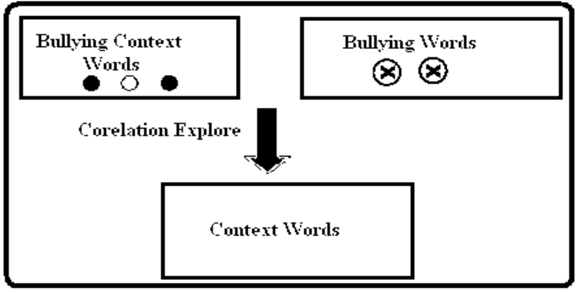


Fig.1.Proposed system structure

3. PROJECTED STRUCTURE:

Within this paper, we investigate one deep learning method named stacked Denoising auto encoder (SDA). SDA stacks several Denoising auto encoders and concatenates the creation of each layer because the learned representation. Additionally, each auto encoder layer is supposed to learn an more and more abstract representation from the input. Within this paper, we create a new text representation model with different variant of SDA: marginalized stacked Denoising auto encoders (mSDA), which adopts straight line rather of nonlinear projection to accelerate training and marginalizes infinite noise distribution to be able to find out more robust representations. Each Denoising auto encoder in SDA is educated to recover the input data from the corrupted form of it. Three types of information including text, user demography, and social networking features are frequently utilized in cyber bullying recognition. Because the text content is easily the most reliable, our work here concentrates on text-based cyber bullying recognition. The input is corrupted by at random setting a few of the input to zero that is known as dropout noise. This Denoising process helps the auto encoders to understand robust representation. We utilize semantic information to grow mSDA and develop Semantic-enhanced Marginalized Stacked Denoising Auto encoders. The semantic information includes bullying words. A computerized extraction of bullying words according to word embeddings is suggested so the involved human labor could be reduced [4]. During training of smSDA, we try to rebuild bullying features using their company normal words by finding the latent structure, i.e. correlation, between bullying and normal words. The intuition behind this concept is the fact that some bullying messages don't contain bullying words. The correlation information discovered by smSDA helps you to rebuild bullying features from normal words, and therefore facilitates recognition of bullying messages without that contains bullying words. Benefits of suggested system: The brand new feature space can enhance the performance of cyber bullying recognition despite a little labeled training corpus [5]. Semantic details are integrated into the renovation process through the designing of semantic dropout noises and imposing sparsity constraints on mapping matrix. Within our framework, high-quality semantic information, i.e., bullying words, could be extracted instantly through word embeddings. Finally, these specialized modifications result in the new feature space more discriminative and therefore facilitates bullying recognition. An extensive try real-data sets have verified the performance in our suggested model.

Enhanced Auto-Encoder: Within our suggested smSDA, the sparsity constraint is recognized through the incorporation of L1 regularization term in to the objective work as within the lasso problem. The co-occurrence information has the capacity to derive a strong feature representation under an without supervision learning framework, this motivates other condition-of-the-art text feature learning methods for example Latent Semantic Analysis and subject models. In cyber bullying recognition, most bullying posts contain bullying words for example profanity words and foul languages. These bullying test is very predictive of the presence of cyber bullying.

Our suggested smSDA can cope with the issue by learning a strong feature representation that is a higher level concept representation. For that lower layer, expert understanding and word embeddings are utilized. For that other layers, discriminative feature selection is carried out. Additionally, because the word embeddings adopted listed here are been trained in a sizable scale corpus from Twitter, the similarity taken by word embeddings can represent the particular language pattern. the built bullying features are utilized to train the very first layer within our suggested smSDA [6]. It offers a double edged sword: the first is the initial insulting seeds according to domain understanding and yet another may be the extended bullying words via word embeddings. Here, we adopt a technique known as Iterated Ridge Regression that has been shown to be extremely powerful. Because of the introduced semantic dropout noise, the expected matrices: E [P] and E [Q] is going to be computed slightly different. Within the new space, because of the taken feature correlation and semantic information, the SVM. For cyber bullying problem, we design semantic dropout noise to highlight bullying features within the new feature space, and also the produced new representation is thus more discriminative for cyber bullying recognition. The learned statistical representations can then be given into Support Vector Machine. Most cyber bullying recognition methods depend around the BoW model. A bullying trace is understood to be the response of participants for their bullying experience. Bullying traces include not just messages about direct bullying attack, but additionally messages about reporting a bullying experience, revealing self like a victim. The MySpace dataset is crawled from MySpace groups. Each group includes several posts by different users, which may be considered like a conversation about one subject. For the suggested methods including smSDA and smSDAu: the noise intensity and the amount of layers are going to exactly the same values as with mSDA to provide a good comparison. This paper addresses the written text-based cyber bullying recognition problem, where robust and discriminative representations of messages are crucial for a highly effective recognition system. To judge the performance of those methods on binary classification, classification precision is utilized. Thinking about both datasets possess the class imbalance problem, we introduce F1-Score, that is a balance between precision and recall, to judge the performance of compared approaches [7]. The performance in our approaches continues to be experimentally verified through two cyber bullying corpora from social medias: Twitter and MySpace. Like a next thing we are intending to further enhance the sturdiness from the learned representation by thinking about word order in messages. As examined that the possible lack of labeled training corpus hinders the introduction of automatic cyber bullying recognition, the sizes of coaching corpus are controlled to be really small within our experiments. The outcomes have proven that smSDAu performs slightly worse than smSDA. This can be described because the impartial semantic dropout noise cancels the enhancement of bullying features.

4. CONCLUSION:

With two public real-world cyber bullying firms, we test our proposed improved semantic zed marginalized Denoising Automobile Encoder. Our suggested semantically improved Marginalized Stacked Denoising Auto encoder can effectively and efficiently learn robust features from the BoW representation. This solid properties are used for rebuilding the original details from corruption (i.e. missing) functions. We also developed semantically improved marginalized denoising encoders such as a specialized model of cyber bullying identification by modeling semantic dropout rushing and applying sparsely. Furthermore, word embedding is used to extend and optimize text lists initialized by domain comprehension immediately. Most bullies contain bullying terms such as profanity words and foul languages in cyber bullying awareness. This bullying measure is highly predictive of cyber intimidation. Our proposed someday will address the problem by studying a strong representation of a higher level definition.

REFERENCES:

[1] Rui Zhao and Kezhi Mao, “Cyber bullying Detection based onSemantic-Enhanced Marginalized Denoising Auto-Encoder”, IEEE Transactions on Affective Computing, 2016.

[2] T. H. Dat and C. Guan, “Feature selection based on fisher ratio and mutual information analyses for robust brain computer interface,” in Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, vol. 1. IEEE, 2007, pp. I–337.

[3] T. L. Griffiths and M. Steyvers, “Finding scientific topics,” Proceedings of the National academy of Sciences of the United States of

America, vol. 101, no. Suppl 1, pp. 5228–5235, 2004.

[4] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, “Distributed representations of words and phrases and their compositionality,” in Advances in neural information processing systems, 2013, pp. 3111–3119.

[5] M. Dadvar, F. de Jong, R. Ordelman, and R. Trieschnigg, “Improved cyber bullying detection using gender information,” in Proceedings of the 12th -Dutch-Belgian Information Retrieval Workshop (DIR2012). Ghent, Belgium: ACM, 2012.

[6] M. Ptaszynski, F. Masui, Y. Kimura, R. Rzepka, and K. Araki, “Brute force works best against bullying,” in Proceedings of IJCAI 2015 Joint Workshop on Constraints and Preferences for Configuration and Recommendation and Intelligent Techniques for Web Personalization. ACM, 2015.

[7] M. Ybarra, “Trends in technology-based sexual and non-sexual aggression over time and linkages to nontechnology aggression,” National Summit on Interpersonal Violence and Abuse Across the Lifespan: Forging a Shared Agenda, 2010.

Content-Dependent Visual Extraction Strategy For Similarity Search

Potnuru Lavnya[1]., V G Anupa[2]., B Tejaswini[3]., V.Nikitha[4]., P.Priyanka[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- mail.to.plavanya@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A05A2, 16M51A0518, 16RG1A05A5, 15RG1A05H2),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— LIME is available, one for various organizations' accountable bandwidth. The parties involved, their partnerships, are established and a realistic instantiation is given for every protocol on bandwidth, which employs a modern combination of unclear transmission, powerful watermarking and digital signatures. Within this work we propose a normal LIME data lineage system for multiple individuals with two main functions. In certain cases, detecting a leaker is due to forensic methods, but they are normally pricey and do not necessarily yield the favourite results. We identify the specific security guarantees required by this sort of data lineage process against recognition of the guilty party, and find out the simplifying non-repudiation and integrity assumptions. Then we establish and test a singular responsible bandwidth protocol between two actors within a malicious environment because they build upon oblivious transmission, rigorous watermarking, and signature primitives. Finally, an experimental assessment is performed to show how well our protocol is working and to adapt our method to the main knowledge outsourcing and social systems data leakage scenarios. In general, we believe that LIME, our bandwidth lineage architecture, is a crucial step towards design transparency. It enforces transparency by design, i.e. it leads the engineer to consider potential data leaks and the associated responsibilities restrictions at the design stage.

***Keywords*— Accountability, fingerprinting, oblivious transfer, watermarking, Information leakage, data lineage, public key cryptosystems**

1. INTRODUCTION

Materials like file encryption only have security when information of significant importance is encrypted, so nothing will keep it from publishing decrypted content if the receiver decrypts a note. The dilemma is exacerbated by an increase in social systems and smart phones. In such settings, many providers, commonly known as third-party apps, share their private details to obtain the potentially free websites[1]. We describe LIME, the normal dataset frame for data flow in the malicious environment through multiple entities. We introduce yet another role by means of auditor, whose task would be to determine a guilty party for just about any data leak, and define the precise qualities for communication between these roles. Therefore, we explain the requirement for an over-all accountability mechanism in data transfers. We implement our protocol like a C library: we make use of the pairing-based cryptography library to construct the actual oblivious transfer and signature primitives

2. PREVIOUS DESIGN:

The information provenance methodology, by means of robust watermarking techniques or adding fake data, was already recommended within the literature and utilized by some industries. Hasan et al. present a method that enforces logging of read actions inside a tamper-proof provenance chain. This creates the potential of verifying the foundation of knowledge inside a document. Poh addresses the issue of accountable bandwidth with untrusted senders while using term fair content tracing [2]. He presents an over-all framework to check different approaches and splits protocols into four groups based on their usage of reliable organizations, i.e., no reliable organizations, offline reliable organizations, online reliable organizations and reliable hardware. In addition, he introduces the extra qualities of recipient anonymity and fairness in collaboration with payment. Disadvantages of existing system: Most efforts happen to be ad-hoc anyway and there's no formal model available. Furthermore, many of these approaches only allow identification from the leaker inside a non-provable manner, which isn't sufficient oftentimes. An assailant has the capacity to strip from the provenance information of the file; the issue of information leakage in malicious environments isn't tackled by their approach.

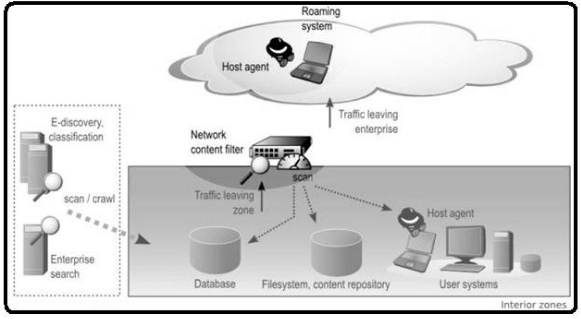


Fig.1.System architecture

3. EXTENDED DESIGN:

Intentional or unintended leakage of private information is unquestionably probably the most severe security threats that organizations face within the digital era. The threat now reaches your own lives: an array of private information can be obtained to social systems and Smartphone providers and it is not directly used in untrustworthy 3rd party and 4th party applications. We explain the requirement for an over-all accountability mechanism in data transfers. In a variety of leakage scenarios [3]. This technique defines LIME, a normal data lineage framework for data flow across multiple entities within the malicious atmosphere. We realize that entities in data flows assume 1 of 2 roles: owner or consumer. We introduce yet another role by means of auditor, whose task would be to determine a guilty party for just about any data leak, and define the precise qualities for communication between these roles. Along the way, we identify an optional non-repudiation assumption made between two proprietors, as well as an optional trust (honesty) assumption produced by the auditor concerning the proprietors. As our second contribution, we produce an accountable bandwidth protocol to verifiably transfer data between two entities. To cope with an untrusted sender as well as an untrusted receiver scenario connected with bandwidth between two consumers; our protocols employ a fascinating mixture of the robust watermarking, oblivious transfer, and signature primitives. Benefits of suggested system: This can help to beat the present situation where most lineage mechanisms are applied once a leakage has happened. We prove its correctness and show that it's realizable by providing micro benchmarking results. By presenting an over-all relevant framework, we introduce accountability as soon as within the design phase of the bandwidth infrastructure.

Preliminaries: We make use of a CMA-secure signature, i.e., no polynomial-time foe has the capacity to forge a signature with non-minimal probability. We must have our watermarking plan to aid multiple re-watermarking, i.e., it ought to permit multiple watermarks to become embedded successively without influencing their individual identifies ability [4]. To supply sturdiness, the watermark is baked into the most important area of the picture, to ensure that taking out the watermark shouldn't be possible without destroying the actual picture. The a-factor from the formula is really a parameter that determines how strong the Gaussian noise is influencing the initial image. Within this context, when talking of learning nothing, we really mean nothing could be learned with non-minimal probability.

Framework of LIME: You will find three different roles that may be allotted to the involved parties in LIME: data owner, data consumer and auditor. When documents are transferred in one owner to a different one, we are able to think that the transfer is controlled by a non-repudiation assumption. To cope with an untrusted sender as well as an untrusted receiver scenario connected with bandwidth between two consumers; our protocols employ a fascinating mixture of the robust watermarking, oblivious transfer, and signature primitives. A method that may offer these qualities is robust watermarking. We provide a meaning of watermarking along with a detailed description from the preferred qualities. Inside a real life setting the auditor could be any authority, for instance a governmental institution, police, a legitimate person or perhaps some software. Within the outsourcing scenario, the business can invoke the auditor who recreates the lineage and therefore uncovers the identity from the leaker [5]. As our only goal would be to identify guilty parties, the attacks we're worried about are individuals that disable the auditor from provably identifying the guilty party. As already pointed out formerly, consumers might transfer a document to a different consumer, so we have to think about the situation of the untrusted sender. Our approach doesn't take into account derived data, because the initial information could be lost throughout the creation procedure for derived data.

Responsible Data Transmission: To do this property, the sender divides the initial document into n parts as well as for each part he creates two differently watermarked versions. Then he transfers certainly one of all these two versions towards the recipient. We make use of a timestamp t to distinctively identify a particular transfer between two parties, and therefore think that no two transfers between your same two parties occur simultaneously. Presuming the correctness from the file encryption, watermarking, signature and oblivious transfer plan, we reveal that for those possible scenarios the guilty party can be established properly. We currently reveal that a recipient cannot cheat throughout the auditing process, as he proves which form of the document he requested for throughout the transfer protocol. False positives within the watermark recognition isn't a major problem, because the probability the correct bit string of length n is spuriously detected is minimal. Normally the recipient might have no chance of realizing this, because he cannot identify the watermark. Because the correctness from the signed statement s is verified within the auditing process and because the sender are only able to forge the recipient's signature with minimal probability, the only real possible ways to mount this attack would be to reuse a legitimate signed statement from the past transaction [6]. We performed the test out different parameters to evaluate the performance. The sender and recipient area of the protocol are generally performed within the same program. The execution time in order to obtain the signatures can also be constant because the number and type of the signed statements is identical for those images. In every protocol run, the sender send two group elements (64 bytes) within the initialization phase. Our work also motivates further research on data leakage recognition approaches for various document types and types of conditions. For instance, it will likely be a fascinating future research direction to create a verifiable lineage protocol for derived data. For any non-blind watermarking plan such as the Cox formula utilized in our implementation the sender must also keep original document. A company functions as owner and may delegate tasks to outsourcing companies which behave as consumers within our model [7]. It's possible the outsourcing companies receive sensitive data to operate on and because the outsourcing information mill not always reliable through the organization, fingerprinting can be used on transferred documents. The internet social networking uses all of this information like a consumer within this scenario. 3rd party applications that get access to these details to acquire some service behave as further consumers within this scenario.

4. CONCLUSION:

We prove its accuracy and demonstrate that the effects of micro-benchmarking can be achieved. We add responsibility as soon as we are in the design stage of the bandwidth networks by proposing an overall relevant context. While LIME does not deter data leakage in a positive manner, it introduces responsiveness. It can also prevent dishonest parties from dropping private documents and will enable honest parties to ensure that confidential data is safeguarded. When we discriminate between trustworthy senders and entrusted senders, LIME is versatile. Within the situation from the reliable sender, a simple protocol with little overhead can be done. This accountability could be directly connected with provably discovering a transmission good reputation for data across multiple entities beginning from the origin. This is whets called data provenance, data lineage or source tracing. Within this paper, We formalize this concern by linking the guilty party with the leaks, reflecting on methods of communication pathways to address the problem of the leakage of intelligence the untrusted sender wants a more complicated procedure, but the answers are not focused on trusteeship assumptions and can therefore reassure an unpairing entity.

REFERENCES:

[1] Michael Backes, Niklas Grimm, and Aniket Kate, "Data Lineage in Malicious Environments", ieee transactions on dependable and secure computing, vol. 13, no. 2, march/april 2016.

[2] R. Anderson and C. Manifavas, "Chameleon—A new kind of stream cipher," in Proc. 4th Int. Conf. Workshop Fast Softw. Encryption, 1997, pp. 107–113.

[3] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in Proc. 23rd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2003, pp. 145–161.

[4] M. J. Atallah, V. Raskin, C. Hempelmann, M. Karahan, R. Sion, U. Topkara, and K. E. Triezenberg, "Natural language watermarking and tamperproofing," in Proc. Int. Conf. Inf. Hiding, 2002, pp. 196–212.

[5] J.-P. M. Linnartz and M. Van Dijk, "Analysis of the sensitivity attack against electronic watermarks in images," in Proc. Int. Conf. Inf. Hiding, 1998, pp. 258–272.

[6] A. Mascher-Kampfer, H. St€ogner, and A. Uhl, "Multiple re-watermarking scenarios," in Proc. 13th Int. Conf. Syst., Signals, Image Process., 2006, pp. 53–56.

[7] N. P. Sheppard, R. Safavi-Naini, and P. Ogunbona, "Secure multimedia authoring with dishonest collaborators," EURASIP J. Appl. Signal Process., vol. 2004, pp. 2214–2223,

A VIBRANT PLAN TO GET UNIVERSAL RECOGNITION

Valle Kumar Shyam[1]., U Tejasree [2]., Parankusham Susmitha[3] ., Seelam Sanjana[4]., Pusuluri Bindu Manasa[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- vsmca15@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0598, 16RG1A0574, 16RG1A0592, 16RG1A0579),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— Extensive simulation results in connected systems and isolated systems demonstrate that our systems attain high failure rates and occasional false positive rates and low overhead connectivity. The current solution will lead to large amounts of network-wide traffic incompatible with mobile wireless networks with limited sources. The benefit of our approach is that it is essential for linked and disconnected networks. Our solution has similar rates of failure detection, lower overhead contact and much lower false positive rate compared to other techniques using localized control. Our methodology also has the advantage that both linked and disconnected systems are important while centralized control is solely relevant for connected systems. A node which use indoor localization techniques inside an indoor environment in which GPS navigation does not function. In place calculations, various positioning instruments and approaches have different error levels. The risk of failure depends on the node and the environment itself. Our method only produces regional traffic monitoring and is important for linked and disconnected networks In the literature, certain position methods are coded. Ultimately, we achieve an upper limit with our approach to failure detection.

*Keywords— **Node Failure Detection, Localized monitor, FPS, Network Traffic, failure node, disconnected network.***

1. INTRODUCTION

Many current experiments use a structured control technique. One approach It requires any node to send periodic 'Heartbeat' messages to a central monitor, which uses a node malfunction indicator to use the potential absence of heartbeat messages. To control the network, it is important to detect node failures. In this article, we suggest a singular probabilistic approach that incorporates local surveillance, location assessment and node co-operation in order to detect node failures in mobile telephone systems[1]. We recommend two schemes in particular. Node defeats are incredibly difficult to discover on mobile wireless networks because of the highly complex network topology that might not always be connected to the network, and the origins are constrained. This article has a probabilistic method and proposes two systems for the identification of nodes in which localised control, position evaluation and node cooperation are routinely combined. Unfortunately, our strategy could be marginally diminished and the false positive rates could be slightly higher, using centralised control.

Previous Study: They are only applicable to the linked networks as a standard drawback to measure and ACK, heartbeats and gossip-based technologies. A research on localization of high overhead network interface faults uses periodic pings in order to collect information on completed failures between each node set, uses periodic trace routes for the present topology of the network, then passes failures and topology information to a central diagnostic position [2]. Test-and-ACK technology must provide a central display allowing sample messages to be sent to other nodes. The node versatility is known to our method.

2. CLASSICAL METHOD:

One approach adopted by many people existing studies is dependent on centralized monitoring. It takes that every node send periodic “heartbeat” messages to some central monitor, which utilizes the possible lack of heartbeat messages from the node being an indicator of node failure. This method assumes there always exists away from the node towards the central monitor, and therefore is just relevant to systems with persistent connectivity. Another solution depends on localised surveillance, as nodes send heartbeat messages and nodes within the area track each other with heartbeat messages [3]. Only locally monitored traffic is generated and efficiently used in static structures for node failure detection. Present framework drawbacks: If a node A prevents the hearing of hearshaking from another node B, A cannot infer that B has failed because potential cardiovascular signals are not supported by the node B, rather than by a faith in node fai. Where mobile systems are placed, this strategy is influenced by normal ambiguities. Additionally, they result in a lot of network-wide monitoring traffic.

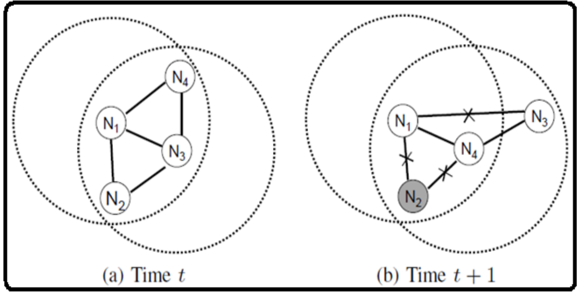


Fig.1.Proposed system architecture

3. ESTIMATED SCHEME:

We advise a singular probabilistic approach that judiciously combines localized monitoring, location estimation and node collaboration to identify node failures in mobile wireless systems. Particularly, we advise two schemes. Within the first plan, whenever a node A cannot listen to a neighboring node B, it uses its very own details about B and binary feedback from the neighbors to determine whether B has unsuccessful or otherwise. Within the second plan, A gathers information from the neighbors, and uses the data jointly to make a decision. The very first plan incurs lower communication overhead compared to second plan [4]. However, the 2nd plan fully utilizes information in the neighbors and may achieve better performance in failure recognition and false positive rates. Benefits of suggested system: Simulation results show both schemes achieve high failure recognition rates, low false positive rates, and incur low communication overhead. When compared with approaches which use centralized monitoring, our approach has as much as 80% lower communication overhead, and just slightly lower recognition rates and slightly greater false positive rates. Our approach has got the advantage that it's relevant to both connected and disconnected systems. When compared with other approaches which use localized monitoring, our approach has similar failure recognition rates, lower communication overhead and far lower false positive rate..

Primitives: When two devices meet, they record the witness information of one another, and exchange the witness information recorded earlier. There's also multiple sinks along with a manager node in the region the sinks are attached to the manager node. We think about a discrete-time system using the time unit of seconds. Each node broadcasts heartbeat packets. the very first application, several automatic sensor nodes, relocates a place to identify hazardous materials. The second reason is searching-and-save application for hikers in backwoods areas. The failure probability depends upon the node itself along with the atmosphere. Many localization techniques happen to be coded in the literature. In the finish, we produce an upper bound of failure recognition rate using our approach. we assume no packet losses which each node has got the same circular transmission range. Within the fundamental situation, a node transmits just one heartbeat packet each and every time. Within an indoor atmosphere where Gps navigation doesn't work, a node may use indoor localization techniques. Different location devices and methods have different amounts of error in location measurements [5]. The intersection of the aforementioned two circles is shaded, addressing the location. Our approach is robust towards the errors in estimating pd and pc, as confirmed by our simulation results. When utilizing our approach, an essential condition for that failure of the to become detected is the fact that there is a minimum of one live node within the transmission selection of A sometimes t. Hence we call them binary and non-binary feedback schemes, correspondingly. To prevent multiple nodes broadcast inquiry messages about B, we assume A starts a timer having a random timeout value, and just broadcasts a question message about B once the timer occasions out along with a hasn't heard any query about B. The non-binary feedback plan is different from the binary version for the reason that An initial gathers non-binary information from the neighbors after which calculates the conditional probability that B has unsuccessful using all the details jointly [6]. Generally, once the packet loss rates are low, it's beneficial to make use of the binary plan because of its lower communication overhead we evaluate our schemes with three mobility models: the random waypoint model, the graceful random model and also the Levy walk model. Additionally, we assume homogeneous node failure probability and packet loss probability. We remark our schemes don't have these assumption. We compare our plan to 2 schemes, known as centralized and localized schemes. A supervisor node is incorporated in the central region from the area. Node failure alarms are delivered to the manager node. Balance lower false positive rate under our plan is due to being able to differentiate a node failure in the node leaving the transmission range, as the localized plan cannot differentiate both of these cases. This signifies the tradeoffs between schemes which use centralized monitoring and individuals using localized monitoring. Not surprisingly, the communication overhead decreases when growing the heartbeat interval. However, once the heartbeat interval is big, inaccurate location estimation results in more queries and responses in addition to more messages towards the manager node [7].

4. CONCLUSION:

The benefit of our approach is that it is essential for linked and disconnected networks. Our solution has similar rates of failure detection, lower overhead contact and much lower false positive rate compared to other techniques using localized control. We also developed two node failure recognition systems that integrate localized tracking, position estimation and node coordination for mobile wireless systems with a probabilistic approach. Another solution relies on a decentralized surveillance, in which nodes send heartbeat messages to one-Hop neighbors and nodes to each other in a community through heartbeat messages. Our solution depends on the location and on how nodes see each other using heartbeat signals. Therefore, If location specifics aren't visible or contact blackouts can be noticed, this doesn't work. Efficient strategies for scenarios remain to be developed for the future. Extensive simulation findings indicate that our systems have high failure detection rates, low false positive rates and occasional overhead contact. We have also seen the compromises of binary input and non-binary structures.

REFERENCES:

[1] RuofanJin, Student Member, IEEE, Bing Wang, Member, IEEE, Wei Wei, Member, IEEE,Xiaolan Zhang, Member, IEEE, Xian Chen, Member, IEEE,Yaakov Bar-Shalom, Fellow, IEEE, Peter Willett, Fellow, IEEE, “Detecting Node Failures in Mobile WirelessNetworks: A Probabilistic Approach”, IEEE Transactions on Mobile Computing, 2016.

[2] C. Bettstetter. Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks. In Proc. of ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pages 19–27, New York, NY, USA, 2001. ACM.

[3] D. Liu and J. Payton. Adaptive Fault Detection Approaches for Dynamic Mobile Networks. In IEEE Consumer Communications and Networking Conference (CCNC), pages 735–739, 2011.

[4] I. Rhee, M. Shin, S. Hong, K. Lee, S. J. Kim, and S. Chong. On the Levy-Walk Nature of Human Mobility. IEEE/ACM Transactions on Networking (TON), 19(3):630–643, 2011.

[5] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad hoc Network Routing Protocols. In Proc. of MobiCom, pages 85–97, New York, NY, USA, 1998. ACM.

[6] M. B. McMickell, B. Goodwine, and L. A. Montestruque. Micabot: A robotic platform for large-scale distributed robotics. In Proc. of IEEE International Conference on Robotics and Automation (ICRA), 2003.

[7] R. Badonnel, R. State, and O. Festor. Self-configurable fault monitoring in ad-hoc networks. Ad Hoc Networks, 6(3):458–473, May 2008.

DESIGNING A ANCIENT TO VERIFY THE CONSISTENCY AND APTITUDE OF OUTSOURCED DATA

Gopaji Monica[1]., Sakshi Bhansali[2]., R.Likhitha[3]., R Harshitha[4]., P.Maneesha[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- moni.gopaji123@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0587, 16RG1A0586, 16RG1A0582, 16RG1A0578),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— We build a special authenticated structure called Homomorphic Authenticated Tree in comparison to existing authenticated structures, such as skip list and Merkle tree Additional PoS and dynamic PoS knowledge is available. If a checker wishes to assess the completeness of the file, he altered the block indexes and forwarded these indexes to the cloud server. No current complex PoSs embraces this approach to the best of our knowledge. We also created a new tool known as Cap, an outstanding structure of authentication. We proposed the excellent needs of multi-user cloud storage services and implemented the complex form of PoS. There can't be generalized current dynamic POSs to a multi-user world. The current scheme cannot be applied to the complex PoS, because of structure variability and Tag generation. An operating multi-user cloud storage system needs the secure client-side mix-user deduplication technique, which enables a person to skip the uploading process and acquire the possession from the files immediately, when other proprietors of the identical files have submitted these to the cloud server. to lessen the communication cost both in the evidence of storage phase and also the deduplication phase concentrating on the same computation cost. We illustrate the protection of our buildings and the scientific study and testing findings indicate that our architecture is used effectively. In this article, we present the concept of duplicate dynamic storage proofs, and suggest a competent design called DeyPoS, which is aimed at achieving dynamic PoS and stable mix user deduplication simultaneously.

***Keywords*— Homomorphic Authenticated Tree (HAT), Cloud storage, dynamic proof of storage, deduplication.**

1. INTRODUCTION

The files kept on the server should not be filled out by users. Many businesses, such as Amazon.com, Google, and Microsoft, have cloud computing systems that are their own and that enable users to transfer their files to a website by accessing them and sharing them all with other computers. When a customer outsources its files into cloud storage, data confidentiality is one of the most important qualities. The customer must import all files on the cloud platform for verification, which include massive communication charges, as traditional methods for defending data privacy, such as Message authentication (MAC) codes and digital signatures. They are not ideal for computing facilities in the cloud[1]. The cloud service returns the blocks with their tags on the basis of these challenged indexes. The block integrity and index correctness are verified by the verifier. Dynamic PoS, however, does not encrypt block indexes as a tag, as dynamic activities can alter many unaudited block indexes, resulting in unnecessary computation and communication costs. In the multi-user atmosphere, dynamic PoS needs to be enhanced, as mix-user deduplication is based on the client-side. Although scientific study has suggested many dynamic PoS schemes in single user environments, the issue in multi-user environments is not investigated sufficiently. Dynamic Evidence of Storage (PoS) is really a helpful cryptographic primitive that allows a person to determine the integrity of outsourced files and also to efficiently update the files inside a cloud server. The previous could be directly guaranteed by cryptographic tags. How to approach the second may be the major distinction between PoS and dynamic PoS. In the majority of the PoS schemes , the block index is “encoded” into its tag, meaning the verifier can look into the block integrity and index correctness concurrently. This signifies that users can skip the uploading process and acquire the possession of files immediately, as lengthy because the submitted files already appear in the cloud server [2]. This method can help to eliminate space for storage for that cloud server, and save transmission bandwidth for users. To the very best of our understanding, there are no dynamic PoS that may support secure mix-user deduplication. There are two challenges to be able to solve this issue. On a single hands, the authenticated structures utilized in dynamic PoSs, However, even when mix-user deduplication is achieved , private tag generation continues to be challenging for dynamic operations. In the majority of the existing dynamic PoSs, a tag employed for integrity verification is generated through the secret key from the up loader. Thus, other proprietors who've the possession from the file but haven't submitted it because of the mix-user deduplication around the client-side, cannot produce a new tag once they update the file. In cases like this, the dynamic PoSs would fail. For solving private tag generation, each owner can generate its very own authenticated structure and upload the dwelling towards the cloud server, meaning the cloud server stores multiple authenticated structures for every file. The main approaches PoS and dynamic PoS schemes are homomorphic Message Authentication Codes and homomorphic signatures. With the aid of homomorphism, the messages and MACs/signatures during these schemes could be compressed right into a single message along with a single MAC/signature. Therefore, the communication cost could be dramatically reduced. Deduplication during these scenarios would be to deduplicate files among different groups. Regrettably, these schemes cannot support deduplication because of structure diversity and tag generation. Within this paper, we think about a more general situation that each user features its own files individually. Hence, we concentrate on a deduplicatable dynamic PoS plan in multiuser environments.

2. PREVIOUS METHOD:

In the majority of the existing dynamic PoSs, a tag employed for integrity verification is generated through the secret key from the uploaded. Thus, other proprietors who've the possession from the file but haven't submitted it because of the mix-user deduplication around the client-side, cannot produce a new tag once they update the file. In cases like this, the dynamic PoSs would fail. Haleviet al. introduced the idea of evidence of possession that is a solution of mix-user deduplication on the customer-side. It takes the user can create the Merkle tree with no the aid of the cloud server, which is a big challenge in dynamic PoS [3]. Pietro and Sorniotti suggested another evidence of possession plan which increases the efficiency. Xu etal. suggested a customer-side deduplication plan for encrypted data, however the schema employs a deterministic proof formula which signifies that each file includes a deterministic short proof. Thus, anyone who obtains this proof can pass the verification without possessing the file in your area. Disadvantages of existing system: All existing approaches for mix-user deduplication around the client-side specified for static files. When the files are updated, the cloud server needs to regenerate the entire authenticated structures of these files, which in turn causes heavy computation cost around the server-side. Regrettably, these schemes cannot support deduplication because of structure diversity and tag generation.

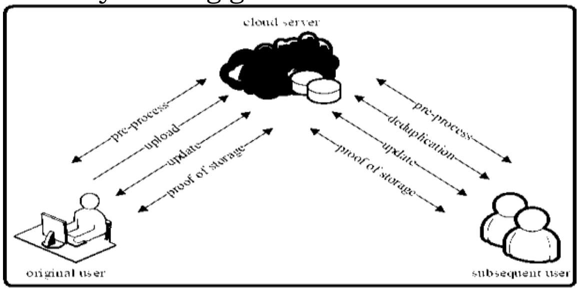


Fig.1.System architecture

3.HOMOMORPHIC AUTHENTICAT-ED TREE:

To the very best of our understanding, this is actually the first try to introduce a primitive known as deduplicatable dynamic Evidence of Storage, which solves the dwelling diversity and tag generation challenges. As opposed to the present authenticated structures, for example skip list and Merkle tree, we design a singular authenticated structure known as Homomorphic Authenticated Tree (HAT), to lessen the communication cost both in the evidence of storage phase and also the deduplication phase concentrating on the same computation cost. Observe that HAT supports integrity verification, dynamic operations, and mix-user deduplication with higher consistency. We advise and implement the very first efficient construction of deduplicatable dynamic PoS known as Dey-PoS, which assists limitless quantity of verification increase operations. The safety of the construction is demonstrated within the random oracle model, and also the performance is examined theoretically and experimentally. Benefits of suggested system: It's an efficient authenticated structure. It's the first practical deduplicatable dynamic PoS plan known as DeyPoS and demonstrated its peace of mind in the random oracle model. The theoretical and experimental results reveal that our DeyPoS implementation is efficient, Performs better particularly when the quality and the amount of the challenged blocks are large.

System Framework: No trivial extension of dynamic PoS is capable of mix-user deduplication. To fill this void, we present a singular primitive known as deduplicatable dynamic evidence of storage. Our body’s model views two kinds of entities: the cloud server and users, for every file, original user may be the user who submitted the file towards the cloud server, while subsequent user may be the user who demonstrated the possession from the file but didn't really upload the file towards the cloud server [4]. You will find five phases inside a deduplicatable dynamic PoS system: pre-process, upload, deduplication, update, and evidence of storage. Within the pre-process phase, users plan to upload their local files. Within the upload phase, the files to become submitted don't appear in the cloud server. The initial users encode the neighborhood files and upload these to the cloud server. Within the deduplication phase, the files to become submitted already appear in the cloud server. The following users hold the files in your area and also the cloud server stores the authenticated structures from the files. Subsequent users have to convince the cloud server they own the files without uploading these to the cloud server. Observe that, these 3 phases are performed just once within the existence cycle of the file in the outlook during users. The cloud server and users don't deal with one another. A malicious user may cheat the cloud server by claiming that it features a certain file, however it really doesn't have it or only offers areas of the file. A malicious cloud server may attempt to convince users it faithfully stores files and updates them, whereas the files are broken or otherwise up-to-date. The aim of deduplicatable dynamic PoS would be to identify these misbehaviors with overwhelming probability. Given personal files, each user that has the whole original file can acquire exactly the same metadata through the initialization formula and pass the deduplication protocol when the file exists within the cloud server [5]. When a user has submitted the file or passed the deduplication protocol, it may convince the cloud server that her possession from the file, and could delete the file from the local storage. Regardless of who runs the encoding formula and uploads the encoded file towards the cloud server, the consumer can run the update protocol and also the checking protocol anytime without possessing the file in your area, which signifies our model is appropriate to multi-user environments. Within our model, all users possess the ownerships of the identical file individually, and also the update by one user shouldn't modify the other users. This signifies the cloud server should keep original version and also the new version from the file concurrently once the original file has multiple proprietors. It is possible by using version control techniques that our model can certainly integrate. Uncheatability captures the home of authenticity for mix-user deduplication around the client-side.

Implementation: To apply a competent deduplicatable dynamic PoS plan, we design a singular authenticated structure known as homomorphic authenticated tree (HAT). A HAT is really a binary tree by which each leaf node matches an information block. Though HAT doesn't have any limitation on the amount of data blocks, with regard to description simplicity, we think that the amount of data blocks n is equivalent to the amount of leaf nodes inside a full binary tree [6]. The formula takes as input a HAT as well as an purchased listing of the block indexes, and outputs an purchased listing of the node indexes. We define the brother or sister search formula It requires the road ? as input, and outputs the index group of the brothers and sisters of nodes within the path ?. Observe that, the creation of the brother or sister search formula isn't an purchased list. It always outputs the leftmost one out of the rest of the brothers and sisters. Both skip list and Merkle tree would be the classical structures in dynamic PoSs. Since there's no deduplication plan according to skip list and also the asymptotic performance of skip list is comparable with this of Merkle tree in dynamic PoSs, we simply discuss the Merkle tree within our paper. Merkle tree isn't appropriate for deduplication in dynamic PoS because of the structure diversity. The purpose of HAT would be to lessen the communication cost in Deduplication. we advise a concrete plan of deduplicatable dynamic PoS known as DeyPoS. It includes five algorithms. we simply compare our plan using the Merkle tree based solutions. Since there's no Merkle tree based solution that supports both dynamic PoS and deduplication, we compare our plan using the one according to Merkle tree [7]. The evaluation includes three aspects, such as the cost within the upload phase, the price within the Deduplication phase, and also the cost within the evidence of storage phase. The price within the update phase is comparable to the price within the evidence of storage phase, thus, we don't present the price within the update phase.

4. CONCLUSION:

The original scheme could not be applied to complex PoS because of the issue of structure diversity and tag-generation. We describe the search type for a brother or sister The road? is needed as an input and the index group of nodes within the route is output. Notice that, the search type is not a bought list when you build the brother or sister. This misbehavior can be identified with overwhelming likelihood as a deduplicable complex PS. The left one of the rest of the brothers and sisters is always made. The classical models of dynamic PoSs will be both the skip list and the Merkle tree. We proposed the first functional de, according to HAT. In the random oracle model, we proposed an early functional dynamic dynamic PoS Strategy known as DeyPoS and demonstrated its peace of mind.

REFERENCES:

[1] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS, pp. 355–370, 2009.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. of CCS, pp. 598–609, 2007.

[3] A. Yun, J. H. Cheon, and Y. Kim, “On Homomorphic Signatures for Network Coding,” IEEE Transactions on Computers, vol. 59, no. 9, pp. 1295–1296, 2010.

[4] Kun He, Jing Chen, Ruiying Du, Qianhong Wu, GuoliangXue, and Xiang Zhang, “DeyPoS: Deduplicatable Dynamic Proof ofStorage for Multi-User Environments”, IEEE Transactions on Computers, 2016.

[5] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” in Proc. of CCS, pp. 187–198, 2009.

[6] Z. Ren, L. Wang, Q. Wang, and M. Xu, “Dynamic Proofs of Retrievability for Coded Cloud Storage Systems,” IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2015.

[7] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, “Proofs of ownership in remote storage systems,” in Proc. of CCS, pp. 491–500, 2011.

A CONTROLLED PRECAUTIONARY DESIGN FOR KGA WITH HASH CODES

Thummalagunta Aswani[1]., P.Akanksha [2]., T.Katta Snehitha[3] ., Thota Susmitha[4]., Palle Keerthi[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- aswani.thummalagunta@gmail.com)

2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0572, 16RG1A0595, 16RG1A0596, 16RG1A0573),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— ***The smooth projective hash function, the concept generated by Cramer & Shoppe, is a main component of our two-server, public key encryption file search construction. We must have a different essential property of smooth projective hash functions during this article. We add two games to decide the protection of PEKS chipboard text and trapdoor, namely semanthetic safety against selected keyword attack and differentiate between the ability to determine a keyword attack1. While PEKS systems are free of hidden dissemination, they suffer from a natural vulnerability about the privacy of the trapdoor Keywords, namely inside the Guessing Attack Keyword. Sadly, the traditional PEKS architecture has been developed and is grappling with an all-natural vulnerability known as a malicious server attack. We advise a brand new PEKS system, known as PEKS dual server, to fix this security flaw. The stable DS-PEKS from LH-SPHF must be seen daily. Our PEKS computing strategy is easily the most effective. Since our schedule would not contain combination calculations. Particularly because of two combinations of calculations per PEKS generation, this plan requires the most computational costs.***

Keywords— ***Keyword search, secure cloud storage, encryption, inside keyword guessing attack, smooth projective hash function, Diffie-Hellman language.***

1. INTRODUCTION

In particular, users must securely exchange hidden keys that can be used for the encryption of data files. Otherwise the encrypted cloud data will not be shared. In order to address this problem, Boneh et al. launched a much more versatile primitive, called Public Key File Search encryption, which permits anyone to look at encrypted data under uneven encryption. The PEKS device attaches encrypted keywords by accessing the encrypted data when using the recipient's public key. Typical methods provide searchable file encryption that allows the client to recover encrypted documents using the client's keywords, where the server will reveal information required by using the user inadvertently due to the keyword trapdoor. Searchable file encryption may be recognized both in symmetric or uneven files file encryption setting [1]. The receiver then transmits the trapdoor in the to-be-looked keyword for that server for data searching. Because of the trapdoor along with the PEKS cipher text, the server can test once the keyword underlying the PEKS ciphertext is equivalent to the main one selected using the receiver. If that's the problem, the server transmits the matching encrypted data for that receiver. However, the reality is, finish users might not entirely trust the cloud storage servers and might wish to secure their data before uploading individuals towards the cloud server to be able to safeguard the information privacy. No matter being free of secret key distribution, PEKS schemes experience an all-natural insecurity regarding the trapdoor keyword privacy, namely inside Keyword Guessing Attack (KGA). We formalize a totally new PEKS framework named Dual-Server Public Key File encryption with Keyword Search (DS-PEKS) to handle safety vulnerability of PEKS. We show a regular construction of DS-PEKS when using the suggested Lin-Hom SPHF. A totally new variant of Smooth Projective Hash Function (SPHF), known as straight line and homomorphic SPHF, is introduced for almost any generic construction of DS-PEKS.

Previous Study: The first PEKS plan without pairings was created by Di Crescenzo and Saraswat. The big event arises from Cock’s IBE plan which isn't very practical. The very first PEKS plan needs a secure funnel to supply the trapdoors. To overcome this limitation, Baek et al. suggested a totally new PEKS plan without requiring a great funnel that is actually a good funnel-free PEKS (SCF-PEKS). The concept should be to adding server’s public/private key pair in a PEKS system. The keyword cipher text and trapdoor are generated when using the server’s public key and so just the server (designated tester) is able to perform search. They enhanced the safety model by presenting the adaptively secure SCF-PEKS, in which a foe is permitted to issue test queries adaptively. Byun et al. introduced the off-line keyword guessing attack against PEKS as keywords are selected within the much smaller sized space than passwords and users usually use well-known keywords for searching documents [2]. The first PEKS plan secure against outdoors keyword guessing attacks was suggested by Rhee et al. The idea of trapdoor in distinguish ability was suggested along with the authors proven that trapdoor in distinguish ability could be a sufficient condition to prevent outdoors keyword-guessing attacks. An affordable solution should be to propose a totally new framework of PEKS.

2. CONVENTIONAL APPROACH:

Inside a PEKS system, while using receiver's public key, the sender attaches some encrypted keywords using the encrypted data. The receiver then transmits the trapdoor of the to-be-looked keyword towards the server for data searching. Because of the trapdoor and also the PEKS cipher text, the server can test if the keyword underlying the PEKS cipher text is equivalent to the main one selected through the receiver. If that's the case, the server transmits the matching encrypted data towards the receiver. Baeket al. suggested a ew PEKS plan without requiring a safe and secure funnel, which is called a safe and secure funnel-free PEKS. Rhee et al. later enhanced Baeket al.'s security model for SCF-PEKS in which the attacker is permitted to get the relationship between your non-challenge cipher texts and also the trapdoor. Byun et al. introduced the off-line keyword guessing attack against PEKS as keywords are selected from the much smaller sized space than passwords and users usually use well-known keywords for searching documents [3]. Disadvantages of existing system: The main reason resulting in this type of security vulnerability is the fact that anybody you never know receiver's public key can create the PEKS cipher text of arbitrary keyword them self. Particularly, given a trapdoor, the adversarial server can pick a guessing keyword in the keyword space after which makes use of the keyword to develop a PEKS cipher text. The server then can test if the guessing keyword may be the one underlying the trapdoor. This guessing-then-testing process could be repeated before the correct keyword is located. On a single hands, even though the server cannot exactly guess the keyword, it's still in a position to know which small set the actual keyword is associated with and therefore the keyword privacy isn't well maintained in the server. However, their plan is impractical because the receiver needs to in your area discover the matching cipher text using the exact trapdoor to remove the non-matching ones in the set came back in the server.

3. FORMALIZED SCHEME:

The contributions of the paper are four-fold. We formalize a brand new PEKS framework named Dual-Server Public Key File encryption with Keyword Search (DS-PEKS) to deal with the safety vulnerability of PEKS. A brand new variant of Smooth Projective Hash Function (SPHF), known as straight line and homomorphic SPHF, is introduced for any generic construction of DS-PEKS. We show a normal construction of DS-PEKS while using suggested Lin-Hom SPHF. As one example of the practicality in our new framework, a competent instantiation in our SPHF in line with the Diffie-Hellman language is presented within this paper. Benefits of suggested system: All of the existing schemes require pairing computation throughout the generation of PEKS cipher text and testing and therefore are less capable than our plan, which doesn't need any pairing computation. Within our plan, although we require another stage for that testing, our computation price is really lower compared to any existing plan as we don't require any pairing computation and all sorts of searching jobs are handled through the server.

Implementation: Searchable file encryption is of speeding up interest for shielding the information privacy in secure searchable cloud storage. In relation to trapdoor generation, as all of the existing schemes don't involve pairing computation, the computation price is reduced in comparison with PEKS generation [4]. During this paper, we investigate security in the well-known cryptographic primitive, namely, public key file encryption with keyword search that's very helpful in a number of applying cloud storage. A DS-PEKS plan mainly includes. To obtain more precise, the KeyGen formula generates the general public/personal key pairs from the back and front servers instead of this within the receiver. Within the traditional PEKS, since there's just one server, when the trapdoor generation formula is public, your server can launch a guessing attack against a keyword cipher text to extract the encrypted keyword. Another one of the conventional PEKS and our suggested DS-PEKS may be the test formula is separated into two algorithms, Front Make certain Back Test operated by two independent servers. This is often required for achieving security from the inside keyword guessing attack. Within the DS-PEKS system, upon acquiring a question inside the receiver, the important thing server pre-processes the trapdoor and PEKS cipher texts getting its private key, then transmits some internal testing-states for that back server while using the corresponding trapdoor and PEKS cipher texts hidden. A corner server will pick which documents are queried using the receiver getting its private key along with the received internal testing-states at the front server [5]. You have to understand that both front server along with the back server here needs to be “honest but curious” and won't collude with one another. More precisely, both servers perform testing strictly transporting out an agenda procedures but could be thinking about the specific keyword. We must understand that the next security models also imply the safety guarantees outside adversaries that have less capacity in comparison to servers. We introduce two games, namely semantic-security against selected keyword attack and indistinguishability against keyword guessing attack1 to capture the safety of PEKS ciphers text and trapdoor, correspondingly. The PEKS cipher text doesn't reveal any specifics of the specific keyword for the foe. This security model captures the trapdoor reveals no specifics of the specific keyword for that adversarial front server. Adversarial Back Server: The safety types of SS - CKA and IND - KGA in relation to an adversarial back server become individuals against an adversarial front server. Here the SS - CKA experiment against an adversarial back server is equivalent to the main one against an adversarial front server apart from the foe is supplied the non-public type in the rear server instead of this right in front server. We omit the facts for simplicity. We reference the adversarial back server A within the SS - CKA experiment just as one SS - CKA foe and define its advantage. Similarly, this security model aims to capture the trapdoor doesn't reveal any information for that back server and so is equivalent to that right in front server apart from the foe owns the non-public type in the rear server instead of this right in front server. Within our defined security considered IND-KGA-II, it's crucial the malicious back server cannot learn any specifics of the specific two keywords involved in the internal testing-condition. To begin with, we must understand that both keywords involved in the internal-testing condition plays exactly the same role no matter their initial source Therefore, the job within the foe should be to guess the 2 underlying keywords within the internal testing overuse injury in general, rather for each within the initial PEKS cipher text along with the initial trapdoor. Therefore, it's inadequate for the foe to submit number of challenge keywords and so we must hold the foe to submit three different keywords within the challenge stage and guess which two keywords are selected because of the challenge internal-testing condition. A principal component of our construction for dual-server public key file encryption with keyword search is smooth projective hash function (SPHF), an idea created by Cramer and Shoup. During this paper, we must have another critical property of smooth projective hash functions [6]. Precisely, we must hold the SPHF to obtain pseudo-random. During this paper, we introduce a totally new variant of smooth projective hash function. Our plan's considered because the efficient in relation to PEKS computation. Because our plan doesn't include pairing computation. Particularly, this program necessitates most computation cost because of 2 pairing computation per PEKS generation. In relation to trapdoor generation, as all of the existing schemes don't involve pairing computation, the computation price is reduced in comparison with PEKS generation [7]. You have to note the trapdoor generation within our plans a little more than individuals of existing schemes because of the additional exponentiation computations. You have to understand that this extra pairing computation is carried out across the user side rather within the server. Therefore, it may be the computation burden for users who are able to make use of a simple device for searching data. Within our plan, although we have to have another stage for the testing, our computation price is really lower in comparison with any existing plan once we don't require any pairing computation and searching jobs are handled using the server.

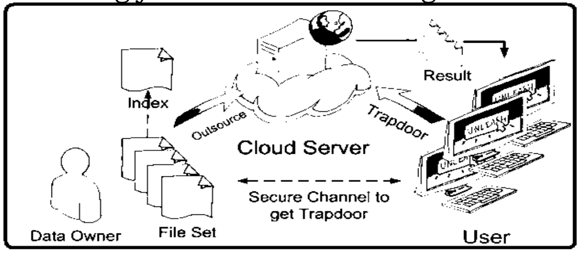


Fig.1.System architecture

4. CONCLUSION:

During this article we proposed a whole new mechanism called Keyword Search (DS-PEKS) encryption of a Public Key File Dual-Server that can lead to the deviations of keywords inside a standard PEKS framework that would be a normal weakness. This extra pairing calculation is performed on the user side rather than on the server. This may then be the estimation responsibility for users who would use a basic data search system. We added a brand new Smooth Projective Hash (SPHF) feature and tried to complete a standard DS-PEKS strategy around the extensor. A stable instantiation within the new SPHF is also presented during the use of the Diffie-Hellman problem, which offers a confident DS-PEKS plan without any pairings. With regard to trapdoor generation, the price of the computation is minimized when compared with PEKS generation because not all current schemes require pairing computation.

REFERENCES:

[1] Rongmao Chen, Yi Mu, Senior Member, IEEE, Guomin Yang, Member, IEEE, FuchunGuo, and Xiaofen Wang, “Dual-Server Public-Key Encryption With KeywordSearch for Secure Cloud Storage”, ieee transactions on information forensics and security, vol. 11, no. 4, april 2016.

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006, pp. 79–88.

[3] C. Cocks, “An identity based encryption scheme based on quadratic residues,” in Cryptography and Coding. Cirencester, U.K.: Springer, 2001, pp. 360–363.

[4] J. Baek, R. Safavi-Naini, and W. Susilo, “On the integration of public key data encryption and public key encryption with keyword search,” in Proc. 9th Int. Conf. Inf. Secur. (ISC), 2006, pp. 217–232.

[5] D. Khader, “Public key encryption with keyword search based on K-resilient IBE,” in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006, pp. 298–308.

[6] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, “Generic constructions of secure-channel free searchable encryption with adaptive security,” Secur. Commun. Netw., vol. 8, no. 8, pp. 1547–1560, 2015.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

AUDIT STATIC ARCHIVE DATA WITH VIBRANT SUPPORTIVE SCHEME

Venkata Seshu Kiran T[1]., Neela Teja [2]., Thaduri Susmitha [3] ., T.Archana [4]., Muppa Supriya [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- seshukiran04@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0566, 16RG1A0594, 16RG1A0597, 16RG1A0562),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— Cloud consumers no longer have their data physically, so it's impossible to ensure the accuracy of external data. Recent proposals for "provable data ownership," for instance, and for "evidence of irretrievability" are made in order to solve this issue, but are not sufficiently supported in terms of the static archive data to be checked. for this reason. In addition, threat models often take on a true data owner and focus on finding a deceptive cloud firm, while customers can even be mistaken. This paper suggests an open auditing plan with support for data dynamics and equal conflict arbitration. In specific, we are developing and efficient handling of complex information by designing a catalogue switch to eliminate the constraint of index use for tag calculations in current systems. We also expand current hazard modeling and introduce a signature sharing concept to establish equal arbitration procedures such that any future conflict is properly resolved to deal with the justice issue to ensuring that no party can misbehave without being identified. The protection review has shown that our scheme is clearly stable and that the success assessment also reveals the overhead complexities of knowledge and conflict arbitration.

***Keywords*— Integrity auditing, public verifiability, dynamic update, arbitration, fairness.**

1. INTRODUCTION

Data audit schemes will allow cloud users to assess the completeness of the remotely stored data without installing them in your so-called check block. Because users no longer have their data physically, and therefore lose direct knowledge power, the direct use of standard cryptographic primitives such as hash- or file encryption can lead to numerous security loopholes [1]. Initially, past audits generally require CSP to establish deterministic evidence by accessing a computer file in its entirety to validate its integrity. Next, some audit systems have private verification that only the data owner has the non-public response to perform the auditing function needs. Thirdly, PDP and POR are planning to audit the scarcely modified static data in such a way that they do not help data dynamics. However, from a general point of view. However, direct extensions of those static data oriented schemes to aid dynamic update could cause other security threats. Upon each update operation, we allocate a brand new tag index for that operating block increase the mapping between tag indices and block indices [2]. Current research usually assumes a genuine data owner within their security models that have an inborn inclination toward cloud users. To deal with the fairness condition in auditing, we introduce another-party arbitrator into our threat model, that is a professional institute for conflicts arbitration and it is reliable and played by data proprietors and also the CSP. We offer fairness guarantee and dispute arbitration within our plan.

2. CLASSIC DESIGN:

To begin with, earlier auditing schemes usually require CSP to develop a deterministic proof by being able to access the entire computer file to do integrity check. Next, some auditing schemes provide private verifiability that needs just the data owner that has the non-public answer to carry out the auditing task, which might potentially overburden the dog owner because of its limited computation capacity. Thirdly, PDP and PoR plan to audit static data which are rarely updated, so these schemes don't provide data dynamics support. But from the general perspective, data update is a type of requirement of cloud applications. Disadvantages of existing system: Supplying data dynamics support is easily the most challenging. It is because most existing auditing schemes plan to embed a block's index into its tag computation, which serves to authenticate challenged blocks. However, when we insert or delete a block, block indices of subsequent blocks can change, then tags of those blocks need to be re-computed [3]. This really is unacceptable due to its high computation overhead. Current research usually assumes a genuine data owner within their security models that have an inborn inclination toward cloud users. However, the truth is, not just the cloud, but additionally cloud users, possesses the motive to take part in deceitful behaviors. In Existing System no integrity auditing plans with public verifiability, efficient data dynamics and fair disputes arbitration. Existing system has got the limitation of index usage in tag computation. In Existing System tag re-computation brought on by block update operations. In Existing System both clients and also the CSP potentially may misbehave during auditing and knowledge update.

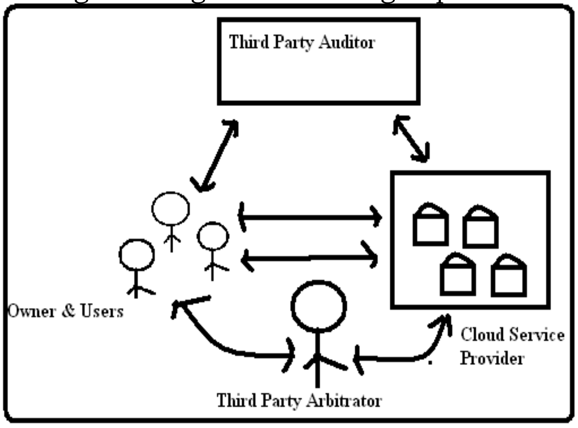


Fig.1.Framework of proposed model

3. VIBRANT DESIGN:

We address this issue by differentiating between tag index and block index, and depend a catalog switcher to keep mapping together. Upon each update operation, we allocate a brand new tag index for that operating block increase the mapping between tag indices and block indices. This type of layer of indirection between block indices and tag indices enforces block authentication and avoids tag re-computation of blocks following the operation position concurrently. Consequently, the efficiency of handling data dynamics is greatly enhanced. In addition and important, inside a public auditing scenario, an information owner always delegates his auditing tasks to some TPA who's reliable through the owner although not always through the cloud. Our work also adopts the thought of signature exchange to guarantee the metadata correctness and protocol fairness, so we focus on mixing efficient data dynamics support and fair dispute arbitration right into a single auditing plan. To deal with the fairness condition in auditing, we introduce another-party arbitrator(TPAR) into our threat model, that is a professional institute for conflicts arbitration and it is reliable and played by data proprietors and also the CSP. Since a TPA may very well be a delegator from the data owner and isn't always reliable through the CSP, we differentiate between your roles of auditor and arbitrator [4]. Furthermore, we adopt the thought of signature exchange to make sure metadata correctness and supply dispute arbitration, where any conflict about auditing or data update could be fairly arbitrated. Generally, this paper proposes a brand new auditing plan to deal with the issues of information dynamics support, public verifiability and dispute arbitration concurrently. Benefits of suggested system: The suggested system solves the information dynamics condition in auditing by presenting a catalog switcher to help keep a mapping between block indices and tag indices, and get rid of the passive aftereffect of block indices in tag computation without incurring much overhead. The suggested system extend the threat model in current research to supply dispute arbitration, that is of effective significance and functionality for cloud data auditing, because most existing schemes generally assume a genuine data owner within their threat models. The suggested system provides fairness guarantee and dispute arbitration within our plan, which helps to ensure that both data owner and also the cloud cannot misbehave within the auditing process otherwise it is simple for any third-party arbitrator to discover the cheating party.

Preliminaries: Cloud users depend around the CSP for data storage and maintenance, plus they may access increases their data. To ease their burden, cloud users can delegate auditing tasks towards the TPAU, who periodically performs the auditing and honestly reports the end result to users. The CSP makes gain selling its storage ability to cloud users, so he's the motive to reclaim offered storage by deleting rarely or never utilized data, as well as hides loss of data accidents to keep a status [5]. We extend the threat model in existing public schemes by differentiating between your auditor (TPAU) and also the arbitrator (TPAR) and putting different trust assumptions in it. Our design goal is, Fair dispute arbitration: to permit a 3rd party arbitrator to fairly settle any dispute about proof verification and dynamic update, and discover the cheating party.

Our Implementation structure: Our dynamic auditing plan with public verifiability and dispute arbitration includes the next algorithms. Therefore, disputes backward and forward parties are inevitable to some extent. Within our design, we have no additional requirement around the data to become stored on cloud servers. Within our construction, tag indices are utilized in tag computation only, while block indices are utilized to indicate the logical positions of information blocks. In implementation, a worldwide monotonously growing counter may be used to produce a new tag index for every placed or modified block. To be sure the correctness from the index switcher and additional the fairness of dispute arbitration, signatures around the updated index switcher need to be exchanged upon each dynamic operation. However, if parallelization strategy is accustomed to optimize the tag generation and proof verification in the client side, then your access from the index switcher can be a bottleneck of performance. A fundamental truth is that whenever the customer initially uploads his data towards the cloud, the cloud must run the Commitment to determine the validity of outsourced blocks as well as their tags, and later on their signatures around the initial index switcher are exchanged. An easy strategy is to allow the arbitrator(TPAR) make a copy from the index switcher [6]. Furthermore, since the change from the index switcher is because data update operations, the CSP can re-construct the most recent index switcher as lengthy as necessary update information are delivered to the CSP upon each update, which helps the CSP to determine the client's signature and generate their own signature around the updated index switcher. The safety of the protocol depends on the safety from the signature plan accustomed to sign the index switcher, that's, all parties only has minimal probability to forge a signature signed using the other party's private key. Once the client finds failing of proof verification throughout an auditing, he contacts the TPAR to produce an arbitration. To attain stateless arbitration in the TPAR, throughout an arbitration, all parties needs to send his form of the index switcher towards the TPAR for signature verification. Within our arbitration protocol, all parties must send his signature around the latest metadata to another party. We proceed by including several models of update and signature exchange. Now we evaluate the problem in which the signature exchange cannot be normally finished. To optimize looking here we are at tag indices, we sort the indices of challenged blocks before searching. However, data update and dispute arbitration involve the computation and verification from the signature around the index switcher. In implementation, we write the information from the index switcher right into a apply for storage [7]. Thus, computing or verifying the signature around the index switcher must read its content in the file. However in cloud atmosphere, remotely stored data might not simply be read but additionally be updated by users that are a common requirement. To get rid of the index limitation of tag computation in original PDP plan and steer clear of tag re-computation introduced by data dynamics.

4. CONCLUSION:

The purpose of this paper would be to offer an integrity auditing plan with public verifiability, efficient data dynamics and fair disputes arbitration. To eradicate the restriction of the index use for tag measurement and to adequately help dynamics, we separate block indexes from tag indices and plan a catalogue switch to retain the index mapping of block tags to avoid tag recompilation by block update operations that require small overall expenses, as demonstrated in our performance appraisal. Meanwhile, as both clients and the CSP can misbehave during audits and information updates, we are expanding the current threat model to include equal arbitration in the light of current research to settle conflicts between clients and the CSP which is necessary for the usage and promotion of cloud audit systems. We do this by developing protocols for the arbitration according to the principle of sharing metadata signatures for any update process. Our experiments show that our proposed proposal has an efficient overall cost for updating and resolution of disputes.

REFERENCES:

[1] HaoJin, Hong Jiang, Senior Member, IEEE, and Ke Zhou, "Dynamic and Public Auditing with Fair Arbitrationfor Cloud Data", ieee transactions on cloud computing 2016.

[2] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proc. ACM Symp. Applied Computing (SAC 11), 2011, pp. 1550–1557.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. 22nd Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT03), 2003, pp. 416–432.

[4] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote data checking for network coding-based distributed storage systems,” in Proc. ACM Cloud Computing Security Workshop (CCSW 10), 2010, pp. 31–42.

[5] T. S. Schwarz and E. L. Miller, “Store, forget, and check: Using algebraic signatures to check remotely administered storage,” in Proc. IEEE Intl Conf. Distributed Computing Systems (ICDCS 06), 2006, pp. 12–12.

[6] Z. Hao, S. Zhong, and N. Yu, “A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,” IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, pp. 1432–1437, 2011.

[7] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” in Proc. 17th Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT98), 1998, pp. 591–606.

A SUBSTANTIATION TRUST PROPOSAL FOR REAL-INSTANT SERVICES IN UNTIE NET

Sagarika Saka[1]., Ora Shreya [2]., R.Swetha [3] ., Y.Himaja [4]., P.Vyshnavi [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India ✉:- sagarika.547@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0567, 16RG1A0584, 16RG1A05B0, 16RG1A0571),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— In this paper we determine a feature descriptor which uses Local directional number for face analysis, which will recognize the face and the feature. LDN encodes information of the face's structure in a simple and compact way, producing discriminative code than current methods. We calculate the structure of each small pattern with the aid of a compass mask that extracts directional information, and we encode such information using the direction indices (directional numbers) and sign—which will allows us to distinguish among similar patterns related to the structure that have different intensities. The face is analyzed by dividing it into several regions and extract the LDN features from them. Then, we combine the features into the form of a vectorand use it for the face analysis and for the face descriptor. We perform this under several factors which have the intensity ,noise and expressions. Moreover, we test our descriptor with different masks to analyze its performance indifferent face analysis tasks.

Keywords— Fine-grained, two-factor, access control, Web services.

1. INTRODUCTION

The benefits of web-based cloud computing are enormous, such as flexibility, lower cost and capital investments, high operating efficiency, scalability, mobility and prompt marketing for you. First, login is essential when you use the cloud services or have the option to view confidential data in the cloud. Your regular account/password setup would have 2 problems. First of all, conventional authentication based on account/password does not protect the privacy[1]. 1 Each user contains in the authority a user hidden form. When we think about what is said above, it is very popular for many people, especially in some big businesses or organizations, to share computers on web-based services. We advise an excellent-grained two-factor access control protocol for web-based cloud-computing services, having a lightweight security device. By using this device, our protocol provides a two-FA security. First the client secret is needed. The client may be granted access only when he's both products. Furthermore, the client cannot use his secret key with another device of others for the access. Our protocol supports fine-grained attribute-based access which provides an excellent versatility for the system to create different access policies based on different scenarios. By using two-FA, users may have more confidence to make use of shared computers to login for web-based e-banking services. For the same reason, it will be better to get a two-FA system for users within the web-based cloud services to be able to enhance the security level within the system [2]. Concurrently, the privacy within the user can also be preserved. The cloud system only understands that the client offers some needed attribute, whilst not the specific identity within the user.

2. TRADITIONAL METHOD:

Mediated cryptography was initially introduced as a means to allow immediate revocation of public keys. The fundamental concept of mediated cryptography is by using an on-line mediator for each transaction. This on-line mediator is known a SEM since it possesses a charge of security abilities. When the SEM doesn't cooperate then no transactions using the public key are possible any more. Temporary secrets will be refreshed at discrete periods of time via interaction between your user and also the base as the public key remains unchanged through the duration of the machine. Disadvantages of existing system: Key-insulated cryptosystem requires all users to update their keys in each and every period of time. The important thing update process necessitates the security device. When the key continues to be updated, the signing or understanding formula doesn't need the unit any longer within the same time frame period. It's quite common to talk about a pc among differing people. It might be simple for online hackers to set up some spy ware to understand the login password on the internet-browser. The foe functions because the role from the cloud server and tries to discover the identity from the user it's getting together with. Access without Secret Key: The foe attempts to connect to the system with no secret key. It may have its very own security device.

3. ENHANCED MODEL:

The unit has got the following qualities: (1) it may compute some lightweight algorithms, e.g. hashing and exponentiation and (2) it's tamper resistant, i.e., the assumption is that no-one can break intuit to obtain the secret information stored inside. Within this paper, we advise an excellent-grained two-factor access control protocol for web-based cloud-computing services, utilizing a lightweight security device [3]. The unit has got the following qualities. It may compute some lightweight algorithms, e.g. hashing and exponentiation which is tamper resistant, i.e., the assumption is that no-one can enter it to obtain the secret information stored inside. In addition, the consumer cannot use his secret key with another device owned by others for that access. The cloud system only recognizes that the consumer offers some needed attribute, although not the actual identity from the user. To exhibit the functionality in our system, we simulate the prototype from the protocol. Benefits of suggested system: Our protocol supports fine-grained attribute-based access which supplies an excellent versatility for that system to create different access policies based on different scenarios. Simultaneously, the privacy from the user can also be preserved. The cloud system only recognizes that the consumer offers some needed attribute, although not the actual identity from the user. To exhibit the functionality in our system, we simulate the prototype from the protocol. Tamper-resistance. The information stored within the security system is not accessible nor modifiable once it's initialized. Additionally, it'll always stick to the formula specs. Capacity. It is capable of doing look at a hash function. Additionally, it may generate random figures and compute exponentiations of the cyclic group defined more than a finite field. Presented a brand new 2FA access control system for web-based cloud-computing services. 2FA access control system continues to be identified not only to let the cloud server to limit the use of individual's users with similar group of attributes but additionally preserve user privacy.

Preliminary Design: Our access control mechanism is dependent upon expressing the attribute predicate as being a monotone span program. Every monotone Boolean function may be symbolized with a few monotone span program, along with a large class includes compact monotone span programs. We briefly review a signature plan known as BBS. It's connected getting several signature schemes, often known as CL-signatures. BBS is existentially unforgivable against adaptive selected message attack underneath the q-SDH assumption. A naive thinking to attain our goal is to use a normal ABS and just split the client secret key in to a two pronged sword [4]. One part is stored using the user (stored inside the pc) while another part is initialized towards the security device. Additional care needs to be taken in route since normal ABS doesn't make certain the leakage of area of the secret key does not have effect on the safety within the plan during two two-FA, the attacker might have compromised among the factors. We introduce extra unique information stored inside the safety device. The authentication process requires this bit of information combined with user secret key. It's guaranteed that missing either part cannot enable the authentication pass. There's in addition a linking relationship relating to the user's dental appliance the key factor and so the user cannot use another user's device for the authentication. The communication overhead is minimal along with the computation needed within the method is some lightweight algorithms for example hashing or exponentiation over group GT.2 all of the heavy computations for example pairing are transported out on my pc.

System Attributes: Trustee: It is the reason generating all system parameters and initialize the safety device. Attribute-issuing Authority: It's responsible to create user secret key for every user based on their attributes. User: It's the player making authentication while using the cloud server. Each user includes a secret type in the attribute-issuing authority along with a security device initialized using the trustee. Cloud Company: It offers services to anonymous approved users. It interacts while using the user with the authentication process.

Methodology: We assume the safety device found in our physiques satisfies the next needs. Tamper-resistance. The information stored within the home alarm system is neither accessible nor modifiable once it's initialized. In addition, it'll always continue with the formula specs. Capacity. With the ability to do think about a hash function. In addition, it could generate random figures and compute exponentiations in the cyclic group defined more than a finite field [5]. The unit setup process includes a two pronged sword. The client key generation process includes three parts. First, the client generates his secret and public type in Setup. Your home alarm system is initialized using the trustee in Device Initialization. Finally the attribute issuing authority generates the client attribute secret type in line using the user's attribute in AttrGen. The access authentication process is unquestionably an interactive protocol relating to the user along with the cloud company. Effortlessly, a few-party protocol could be a system for proofs of understanding if someone party thinks another party (known as proverb) indeed knows some "knowledge". For almost any zero-understanding evidence of understanding, her extra property of Zero-understanding: no cheating verifier learns anything apart from (x, y)? R. To show our instantiation of PK1 is honest-verifier zero understanding we simply show construct another simulator S, which is capable of doing outputting the transcript within the whole PK1 on input challenge c [6]. We further assume the claim-predicate? Is selected using the attacker. A rival is pointed out to breach the safety reliance upon authentication, access without security device or access without secret key whether it can authenticate effectively for the predicate. We measure the efficiency inside our protocol by 50 % parts. Partially one, we know the main operations for the authentication protocol.

Security access: The fundamental concept of mediated cryptography is to use an on-line mediator for each transaction. This on-line mediator is known a SEM since it offers a cost of security abilities. When the SEM doesn't cooperate then no transactions while using the public key are possible any longer. Within the SMC system, a person includes a secret key, public key along with an identity. Within the signing or understanding formula, it takes the key factor along with the SEM together. Within the signature verification or file encryption formula, it takes the client public key along with the corresponding identity. Because the SEM is controlled with a specialist who's commonly used to handle user revocation, the authority will not provide any cooperation for virtually any revoked user. Thus revoked users cannot generate signature or decrypt cipher text. The primary reason behind SMC should be to solve the revocation problem. Thus the SME is controlled using the authority. Essentially, the authority ought to be online for each signature signing and cipher text understanding. The client isn't anonymous in SMC. During our physiques, the safety method is controlled using the user. Anonymity can also be preserved. Through performance evaluation, we proven the event is "feasible". Within the signing or understanding formula, it takes the key factor along with the SEM together. Within the signature verification or file encryption formula, it takes the client public key along with the corresponding identity. We leave as future attempt to boost the efficiency and all sorts of nice highlights of the unit. Detailed security analysis ensures that the suggested two-FA access control system achieves probably the most well-loved security needs. The overall concept of key-insulated security ended up being store extended-term keys within the physically-secure but computationally-limited device. Short-term secret keys are stored by users round the effective but insecure device where cryptographic computations occur [7]. Temporary secrets will probably be refreshed at discrete intervals via interaction relating to the users along with the base since the public key remains unchanged with the timeframe from the device. The important thing factor update process necessitates security device. When the key remains updated, the signing or understanding formula doesn't need the system anymore inside the same time frame period. While our concept does require security device each time the client tries to interact with the device.

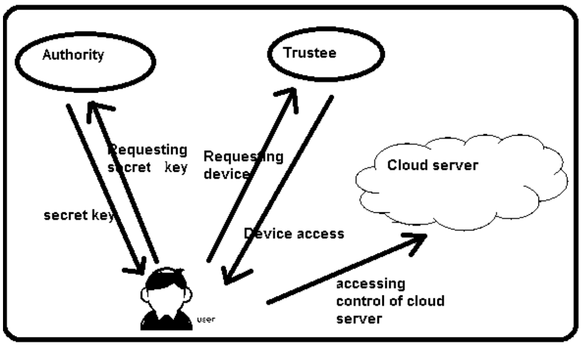


Fig.1.Proposed scheme

4. CONCLUSION:

In web-based e-bank services, 2-FA is very popular. The client will still require a login / password to get a computer to display a password for a single time. Certain systems which require a mobile phone from the user, since the one-time password is transmitted to the phone with the login process via SMS. The Beginning TSetup works by creating public parameters with a trustee. The 2nd component ASetup functions on its Master secret key and public key using the attribute issuing authority. Our protocol provides 2FA protection for this specific unit. Product secrecy is first essential. The protection monitor can also be connected to the server so that the user can authentically enter the cloud. Only when all goods are available should the user be allowed entry.

REFERENCES:

[1] Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang,Rongxing Lu, Senior Member, IEEE, and Jin Li, “Fine-Grained Two-Factor Access Control forWeb-Based Cloud Computing Services”,

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[3] X. Huang et al., “Cost-effective authentic and anonymous data sharing with forward security,” IEEE Trans. Compute., vol. 64, no. 4, pp. 971–983, Apr. 2015.

[4] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, “An efficient PHR service system supporting fuzzy keyword search and fine-grained access control,” Soft Compute., vol. 18, no. 9, pp. 1795–1802, 2014.

[5] T. Okamoto and K. Takashima, “Efficient attribute-based signatures for non-monotone predicates in the standard model,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 35–52.

[6] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, “Security-mediated certificate less cryptography,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.

[7] Y. Dodis and A. Yampolskiy, “A verifiable random function with short proofs and keys,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.

PROTECTED MOBILE PAYMENT MACHINE WITHOUT UTILIZINGCYBER CRIMES

Paramati Chandini[1]., V.Shivani Reddy [2]., P.Ananya [3] ., V.Ashwitha [4]., Y.Aruna Reddy [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- chandinichandu43@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A05A3, 16RG1A0569, 16RG1A05A8, 16RG1A05B2),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— The only problem with a completely off-line solution may be that without a reliable third party, a transaction cannot be prosecuted. In practise, monitoring past purchases without access to third parties or shared accounts will be very difficult, so a vendor finds it difficult to see if digital coins are used. POS machines act as gateways and want to be able to access external charges through processors. It can also be used to modify firmware to overwrite malicious functions. This concept can be used. Techniques of disassembly In addition to the electronic payment system, regarding its nature, PoS Networks manages information that often requires remote control. In this paper, DEDev may be the first approach to include data violation resistance against theft inside a completely offline electronic payment system that does not require credible entities, accounts or stable machines. Our research means DEDev could be the only proposal to use all the qualities needed for a safe micropayment approach while having flexibility in the medium thought payment system. The identity element and the gold medal element are known as handle resistant to the storing and execution of safe and confidential data.

Keywords— Point of Sale (PoS), Mobile secure payment, architecture, protocols, cybercrime, fraud-resilience, Deception Elastic Device (DEDev).

1. INTRODUCTION

The key mechanisms for PoS intrusions are brutally pushing remote access links by using robbed passwords. Yet recent trends suggest the revival of adware and spyware for RAM scraping. Modern PoS systems are computers that have powerful applications equipped with a card reader. The feedback to the PoS is increasingly leveraged by user goods. During the situations, adware and spyware will stolen card data any time the computer is read. Customer coins are not read directly from the networking protocol used by the payment transaction. Instead, the seller only speaks to the aspect of identification, so that the customer is identified[1]. Intensive security monitoring is missing, though, from previous solutions. When focusing on theoretical threats, there is no debate of real-life attacks, such as skimmers, scrapers and vulnerability of intelligence.

Literature Survey: It's worth mentioning here our previous work known as Pressure that, much like DEDev, was built utilizing a PUF based architecture. Actually, monitoring past transactions without any available link with exterior parties or shared databases can be very difficult, because it is hard for a vendor to see if some digital coins happen to be spent [2]. Probably the most relevant variations between and DEDev may be the technology accustomed to compute digital coins. Actually, only one message is distributed in the vendor towards the customer and the other the first is delivered back in the customer towards the vendor that contains all of the needed digital coins, if available. However, the identity element may be used to thwart fraudsters.

2. TRADITIONAL METHOD:

PoS systems serve as portal to a certain network link that allows you to contact the processors of external charging cards. In reality, confirmation of transactions is compulsory. PoS computers may be centrally controlled by some internal networks to reduce costs and ease administration and servicing. To date, proposed mobile payment systems can be found entirely on-line, semi off-line, weak off-line and absolutely off-line. The prior work called FORCE that, much like DEDev, was built utilizing a PUF based architecture. Pressure provided an inadequate prevention strategy according to data obfuscation and didn't address probably the most relevant attacks targeted at threatening customer sensitive data, thus being susceptible to many advanced attack techniques. Disadvantages of existing system: Off-line scenarios are not as easy to safeguard, customer information is stored inside the PoS a lot longer time, thus being more uncovered to attackers. Skimmers: within this attack, the client input device that is one of the PoS products is substituted for an imitation one to be able to capture customer's card data [3]. The primary problem with a completely off-line approach may be the impossibility of examining the standing of a transaction with no reliable 3rd party. Actually, monitoring past transactions without any available link with exterior parties or shared databases can be very difficult, because it is hard for a vendor to see if some digital coins happen to be spent. This is actually the primary reason during last couple of years, a variety of approaches happen to be suggested to supply a reliable off-line payment plan. Although a lot of works happen to be printed, all of them centered on transaction anonymity and gold coin enforceability.

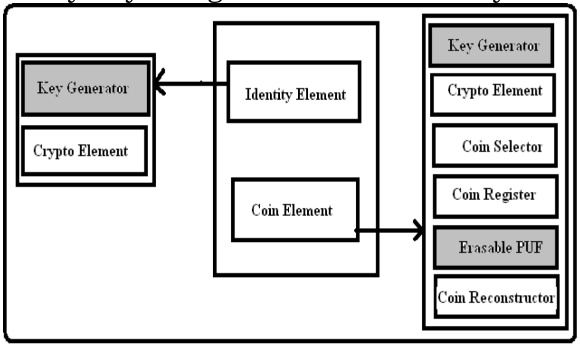


Fig.1.Proposed system architecture

3. ENHANCED METHOD:

Preliminaries: The payment process consists of two primary processing phases, the authorization and also the settlement. PoS system network-level hacking could be made possible by exploiting shared connections, open systems, or by cracking the password from the merchant’s network. Actually, many all-in one PoS system derives from general purpose os's. Off-line scenarios are not as easy to safeguard. In these instances, customer information is stored inside the PoS a lot longer time, thus being more uncovered to attackers. It has been achieved largely by leveraging a singular erasable PUF architecture along with a novel protocol design. In addition, our proposal continues to be completely discussed and compared from the condition from the art. In so doing, the attacker will pressure the payment card data to become in your area processed. Disassembling techniques will also be used with the idea to alter firmwares/softwares in order to replace all of them with malicious functionalities [4]. DEDev may be the first solution that neither requires reliable organizations, nor accounts, nor reliable devices to supply resiliency against frauds according to data breaches inside a fully off-line electronic payment systems. In addition, you should highlight that DEDev continues to be designed to become a secure and reliable encapsulation plan of digital coins. As these process variations aren't controllable during manufacturing, the physical qualities of the device can't be copied or cloned. Even just in fully offline electronic payment systems, this attack continues to be available. Actually, a repayment product is usually composed by several elements and card information is exchanged between these.

Framework: As a result, in instances where customer and vendor are persistently or occasionally disconnected in the network, no secure on-line payment can be done. This paper describes DEDev, a safe and secure off-line micro-payment solution that's resilient to PoS data breaches. Our solution improves over current approaches when it comes to versatility and security. Particularly, we detail DEDev architecture, components, and protocols. Further, an intensive analysis of DEDev functional and security qualities is supplied, showing its usefulness and viability. In addition, by permitting DEDev people to reduce getting a financial institution account causes it to be also particularly interesting with reference to privacy. This paper introduces and discusses DEDev, a safe and secure off-line micro-payment approach using multiple physical unclonable functions (PUFs). DEDev features a name element to authenticate the client, along with a gold coin element where coins aren't in your area stored, but they are computed on-the fly if needed. The communication protocol employed for the payment transaction doesn't directly read customer coins. Finally, some open issues happen to be identified which are left as future work [5]. Particularly, we're investigating the chance to permit digital switch to be spent over multiple off-line transactions while keeping exactly the same degree of security and usefulness. To the very best of our understanding, DEDev may be the first solution that may provide secure fully off-line payments while being resilient to any or all presently known PoS breaches. Rather, the seller only 'talks' to the identity element to be able to find out the user. This simplification alleviates the communication burden using the gold coin element that affected previous approach. Among other qualities, this two-steps protocol enables the financial institution or even the gold coin element issuer to create digital coins to become read only with a certain identity element, i.e., with a specific user. In addition, the identity element accustomed to enhance the security from the users may also be used to thwart malicious users. To the very best of our understanding, this is actually the first solution that may provide secure fully off-line payments while being resilient to any or all presently known PoS breaches. Benefits of suggested system: DEDev continues to be designed to become a secure and reliable encapsulation plan of digital coins. DEDev also relevant to multiple-bank scenarios. Indeed, for debit and credit cards where reliable organizations for example card providers ensure the validity from the cards, some common standard convention may be used in DEDev to create banks capable of producing then sell their very own gold coin element.

Implementation: Differently using their company payment solutions according to tamper-proof hardware, DEDev assumes that just the chips built upon PUFs may take advantage in the tamper evidence feature. The architecture of DEDev consists of two primary elements: a name element along with a gold coin element. A particular gold coin element could be read only with a specific identity element. Both identity element and also the gold coin element are made upon physically unclonable functions. The fundamental 64-sum PUF block first introduced, measures the main difference between two delay terms, each created by the sum of the 64 PUF values. In the initial step the PUF is challenged, thus producing an output along with extra information known as assistant data. Within the next step, the assistant information is accustomed to extract exactly the same output as with the initial step thus making the PUF in a position to build stable values [6]. The gold coin seed register will be used at transaction time for you to challenge the erasable PUF. The acquired fact is combined with gold coin assistant register data to be able to have the original encrypted gold coin again. DEDev depends on standard pairing protocols like the Bluetooth passkey entry simple pairing process. DEDev doesn't provide any transaction dispute protocol. This kind of off-line dispute might be exploited by fraudsters or malicious vendors by injecting fake problems within the transaction or by altering past transactions. Within this paper we've introduced DEDev that's, to the very best of our understanding, the very first data-breach-resilient fully offline micro-payment approach. The safety analysis implies that DEDev doesn't impose trustworthiness assumptions. Further, DEDev can also be the very first solution within the literature where no customer device data attacks could be exploited to compromise the machine. Gold coin seeds and gold coin helpers are written in to the gold coin element registers by the financial institution or gold coin element issuer so that the ultimate gold coin value given as output matches an encrypted form of the actual digital gold coin. Throughout the payment protocol, such tokens will be utilized for an evidence, to authorize the payment process in a manner that the seller can validate, even without connecting for an exterior bank. Choi and Kim aimed to safeguard the keys inside TPMs utilizing a PUF [7]. Actually, once the keys are kept in memory and when they're moved with the bus, their value is altered using the PUF, thus rendering eavesdropping from the PUF IC useless.

4. CONCLUSION:

Actually, DEDev's digital coins are only a digital form of real money and are not thus associated with others in comparison with both the holder and the gold coin. Theft of debit and credit card data is one of the first cybercrimes forms. Even, it is among the most typical nowadays. Attackers are typically built with the intent of the purchasing method, that means the point in which a store first acquires customer data, to rob those customer data. DEDev believes that the fraud data will benefit only from the chips based on PUFs, in comparison to the company's payment solutions utilising tamper-resistant hardware. Our theory is also less stringent than most methods. If the transaction and all types of coins associated with its use appear to go beyond the limits of the proposed protocol, how those coins are to be spent/redempted by the vendor further. The main advantage is that your actors/entities concerned collaborate simpler, quicker and much more securely.

REFERENCES:

[1] Vanesa Daza, Roberto Di Pietro, Flavio Lombardi, and Matteo Signorini, "DEDev: Fraud Resilient Devicefor Off-Line Micro-Payments", ieee transactions on dependable and secure computing, vol. 13, no. 2, march/april 2016.

[2] S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals," in Proc. IEEE Intell. Data Acquisition Adv. Comput. Syst., Sep. 2005, pp. 407–412.

[3] G. Van Damme, K. M. Wouters, H. Karahan, and B. Preneel, "Offline NFC

Payments with Electronic Vouchers," in Proc. ACM 1st ACM Workshop Netw., Syst., Appl. Mobile Handhelds, 2009, pp. 25–30.

[4] R. Battistoni, A. D. Biagio, R. Di Pietro, M. Formica, and L. V. Mancini, "A live digital forensic system for Windows networks," in Proc. 20th IFIP TC Int. Inf. Security Conf., 2008, vol. 278, pp. 653–667.

[5] B. Yahid, M. Nobakht, and A. Shahbahrami, "Providing security for e-wallet using e-cheque," in Proc. 7th Int. Conf. e-Commerce Develop. Countries: Focus e-Security, Apr. 2013, pp. 1–14.

[6] R. Maes, P. Tuyls, and I. Verbauwhede, "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs," in Proc. 11th Int. Workshop Cryptographic Hardware Embedded Syst., 2009, pp. 332–347.

[7] T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited," in Proc. 3rd Int. Conf. Intell. Netw. Collaborative Syst.2011, pp. 656–661.

EXECUTE A DISTINCTIVE ROUTINE FOR REMOTE CHECKING OF DATA INTEGRITY OPEN NETS

Obulesu Damala[1]., M.Vineela [2]., N.Pranupa Reddy [3] ., Pendli Apurva [4]., Yeturu Anitha [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- obulesh.d1231@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0561, 16RG1A0565, 16RG1A0580, 16RG1A05A9),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— This relies on the study findings in proxy cryptography, public key identity and remote cloud data integrity management. This paper focuses in public on proxy-oriented data uploading and remote data integrity checks. In public areas cloud this paper. Our proposed ID-PUIC protocol is successful when using identity based public key cryptography so the administration of the certificate is removed. Actually, the ID-PUIC is a modern, proxy-oriented, public cloud data upload and remote data integrity management model. Customers are relieved of computing burdens across the shared cloud network, universal access to data through geographically independent locations and so forth. The manager should only bind to the network to prevent collusion in the study. But the legitimate business of the boss will be analysed throughout. We include the ID-PUIC protocol with the structured device model and safety model. Then we developed the first concrete ID-PUIC protocol, in conjunction with the bilinear pairings. Our built ID-PUIC protocol is clearly safe inside the random oracle model. However, the proposed ID-PUIC can also carry out private remote data integrity monitoring, delegated remote data integrity control, and public remote data integrity monitoring in accordance with the authorisation of the original client.

Keywords— Proxy public key cryptography, remote data integrity checking, cloud computing, identity-based cryptography.

1. INTRODUCTION

Effective and robust may also be the ID-PUIC protocol. The proposed ID-PUIC protocol will perform private remote data integrity controls, delegated remote data integrity controls and public distant data integrity controls in accordance with the original client permission. Remote monitoring of data privacy in public cloud storage may also be a key safety condition. To help more customers process their data in public cloud sites[1], a new security issue needs to be addressed. Since the customer has been fixed for computer connectivity, he will assign his proxy to process his data and upload it. Cloud computing has been meeting application requirements in recent years and is growing quite rapidly. Thus, a growing number of customers want the remote cloud storage technology to save and process their results. Remote data integrity inspection is also a rudimentary tool to persuade cloud customers to store their data intact. So we will review ID-PUIC protocol in compliance with public encryption based on identity and public key proxy encryption. The manager should only bind to the network to prevent collusion in the study. However, the ethical operation of the manager persists in the study. When you produce a lot of records, who will help you process these data? If the data cannot be stored over time, the manager may be confronted with a lack of financial interest. To avoid the situation happening, the manager needs to delegate the proxy to process its data, for instance, his secretary. But, the manager won't hope others be capable of carry out the remote data integrity checking. Public checking will incur some danger of dripping the privacy. In PKI, the considerable overheads range from heavy certificate verification, certificates generation, delivery, revocation, renewals, etc. In public places cloud-computing, the finish devices might have low computation capacity, for example cell phone, ipad, etc. Identity-based public key cryptography can get rid of the complicated certificate management. To be able to boost the efficiency, identity based proxy-oriented data uploading and remote data integrity checking is much more attractive. In public places cloud, this paper concentrates on the identity-based proxy-oriented data uploading and remote data integrity checking [2]. By utilizing identity-based public key cryptology, our suggested ID-PUIC protocol is efficient because the certificate management is eliminated. ID-PUIC is really a novel proxy-oriented data uploading and remote data integrity checking model in public places cloud. We provide the formal system model and security model for ID-PUIC protocol. Then, in line with the bilinear pairings, we designed the very first concrete ID-PUIC protocol. Within our suggested ID-PUIC protocol, Original Client will communicate with Computers to determine the remote data integrity. An operating ID-PUIC protocol should be efficient and provably secure. In line with the communication and computation overheads, efficiency analysis could be given. To capture the above mentioned security needs, we formalize the safety meaning of an ID-PUIC protocol.

2. PREVIOUS MODEL:

In public places cloud atmosphere, most clients upload their data to Computers and appearance their remote data's integrity by Internet. Once the client is definitely an individual manager, some practical problems may happen. When the manager is suspected to be involved in to the commercial fraud, he'll be removed through the police [3]. Whenever a large of information is generated, who are able to help him process these data. If these data can't be processed just over time, the manager will face the loss of monetary interest. To avoid the situation happening, the manager needs to delegate the proxy to process its data, for instance, his secretary. But, the manager won't hope others be capable of carry out the remote data integrity checking. Chen et al. suggested a proxy signature plan along with a threshold proxy signature plan in the Weil pairing. By mixing the proxy cryptography with file encryption technique, some proxy re-file encryption schemes are suggested. Liu et al. formalize and construct the attribute-based proxy signature. Guoet al. presented a non-interactive CPA-secure proxy re-file encryption plan that is resistant against collusion attacks in forging re-file encryption keys. Disadvantages of existing system: Public checking will incur some danger of dripping the privacy. Less Efficiency. Security level is low.

3. ENHANCED SCHEME:

Increasingly more clients want to store their data to public cloud servers (PCSs) combined with the rapid growth and development of cloud-computing. It can make the clients check whether their outsourced data are stored intact without installing the entire data. In the security problems, we advise a singular proxy-oriented data uploading and remote data integrity checking model in identity-based public key cryptography: identity-based proxy-oriented data uploading and remote data integrity checking in public places cloud (ID-PUIC). We provide the formal definition, system model, and security model [4]. Then, a concrete ID-PUIC protocol was created while using bilinear pairings. The suggested ID-PUIC protocol is provably secure in line with the hardness of computational Diffie-Hellman problem. In line with the original client's authorization, our protocol can realize private checking, delegated checking and public checking. We advise a competent ID-PUIC protocol for secure data uploading and storage service in public places clouds. Bilinear pairings technique makes identity-based cryptography practical. Our protocol is made around the bilinear pairings. We first evaluate the bilinear pairings. Benefits of suggested system: High Quality. Improved Security. The concrete ID-PUIC protocol is probably safe and effective using the formal security proof and efficiency analysis. However, the suggested ID-PUIC protocol may also realize private remote data integrity checking, delegated remote data integrity checking and public remote data integrity checking in line with the original client's authorization. Our suggested ID-PUIC protocol satisfies the non-public checking, delegated checking and public checking. Our contributions will also be appropriate for that scenario of hybrid clouds, in which the proxy may be treatable because the private cloud from the original client. Motivated through the application needs, this paper proposes the novel security idea of ID-PUIC in public places cloud.

Implementation: We advise a competent ID-PUIC protocol for secure data uploading and storage service in public places clouds. Bilinear pairings technique makes identity-based cryptography practical. Our protocol is made around the bilinear pairings. We first evaluate the bilinear pairings. Then, the concrete ID-PUIC protocol was created in the bilinear pairings [5]. Finally, in line with the computation cost and communication cost, we provide the performance analysis from two aspects: theoretical analysis and prototype implementation. Within the paper, we decide the audience G1 which satisfies the problem that CDH issue is difficult but DDH issue is easy. Around the group G1, DDH issue is easy using the bilinear pairings. (G1, G2) will also be known as GDH (Gap Diffie-Hellman) groups. Around the groups G1 and G2, the fundamental requirement would be that the DLP (Discrete Logarithm Problem) is tough. This concrete ID-PUIC protocol comprises four procedures: Setup, Extract, Proxy-key generation, TagGen, and Proof. To be able to show the intuition in our construction, the concrete protocol's architecture is portrayed.

First, Setup is conducted and also the system parameters are generated. In line with the generated system parameters, other procedures are carried out. Within the phase Extract, once the entity's identity is input, KGC generates the entity's private key. Especially, it may create the private keys for that client and also the proxy. Within the phase TagGen, once the data block is input, the proxy generates the block's tag and uploads block-tag pairs to Computers. Within the phase Proxy-key generation, the initial client produces the warrant helping the proxy create the proxy key. Within the phase Proof, the initial client O interacts with Computers. With the interaction, O checks its remote data integrity. First, we provide the computation and communication overhead in our suggested ID-PUIC protocol [6]. Simultaneously, we implement the prototype in our ID-PUIC protocol and evaluate it is time cost. Then, we provide the versatility of remote data integrity checking within the phase Evidence of our ID-PUIC protocol. Finally, we compare our ID-PUIC protocol using the other up-to-date remote data integrity checking protocols. Around the group G1, bilinear pairings, exponentiation, and multiplication lead most computation cost. In contrast to them, another operations are faster, for example, hash function h, the operations on Z* q and G2, etc. The hash function H can be achieved once for those. Thus, we simply consider bilinear pairings, exponentiation, and multiplication on G1. For that proxy, the computation overhead mainly originates from the phase TagGen. Within the phase TagGen, the proxy performs 2n exponentiation, n multiplication around the group G1, and n hash function h. Within the phase Proof, the initial client O generates the task chalk and Computers reacts to chalk. To be able to show our protocol's practical computation overhead, we've simulated the suggested ID-PUIC protocol by utilizing C programming language with GMP Library and PBC library. National Bureau of Standards and ANSI X9 have determined the shortest key length needs: RSA and DSA is 1024 bits, ECC is 160 bits Based on the standard, and we evaluate our ID-PUIC protocol's communication cost. Following the information systems, the block-tag pairs are submitted to Computers for good. Thus, we simply think about the communication cost that is incurred within the remote data integrity checking. Our suggested ID-PUIC protocol satisfies the non-public checking, delegated checking and public checking. Our contributions will also be appropriate for that scenario of hybrid clouds, in which the proxy may be treatable because the private cloud from the original client. Once the original client needs its private cloud carry out the data uploading task, it informs its private cloud [7]. Upon finding the original client's instruction, the non-public cloud will communicate with the general public cloud and finished the information uploading task. The safety in our ID-PUIC protocol mainly includes the next parts: correctness, proxy-protection and enforceability.

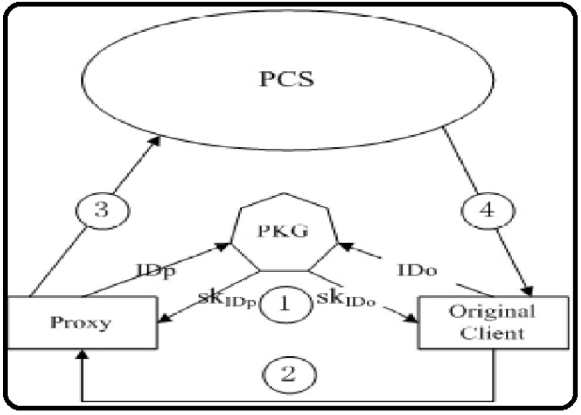


Fig.1.Proposed system

4. CONCLUSION:

In certain special situations, the owner will only log in to the public cloud server, the owner can assign to the third party, as a representative example, the information processor and upload work. On the other hand, the protocol for testing remote data integrity is effective to make it suitable for finishing devices with restricted power. The paper makes the framework and security model of ID-PUIC official. Then, with bilinear pairing technique the very first concrete protocol for ID-PUIC was created. With its systematic security and efficiency review the specific ID-PUIC protocol is likely secure and effective. In PKI, the overhead spectrum for PKI includes heavy credential checks, approvals, shipping, cancellations, renovations, etc. Cloud storage can have low potential for finishing computers, such as mobile phone, ipad, etc. in public areas. The private / public key pair will be provided to the non-public cloud in this case. The non-public cloud receives the proxy key and permission from the original customer for interactions between the original customer and the private cloud.

REFERENCES:

[1] Huaqun Wang, Debiao He, and Shaohua, "Identity-Based Proxy-Oriented Data

Uploading andRemote Data Integrity Checking in Public Cloud", ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.

[2] E. Zhou and Z. Li, "An improved remote data possession checking protocol in cloud storage," in Algorithms and Architectures for Parallel Processing (Lecture Notes in Computer Science), vol. 8631. Berlin, Germany: Springer-Verlag, 2014, pp. 611–617.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Trans. Services Comput., vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.

[4] P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59, no. 32, pp. 4201–4209, 2014.

[5] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2008. [Online]. Available: http://crypto.stanford.edu/pbc/thesis.pdf

[6] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323, 2015.

[7] J. Zhang, W. Tang, and J. Mao, "Efficient public verification proof of retrievability scheme in cloud," Cluster Comput., vol. 17, no. 4, pp. 1401–1411, 2014.

A SEARCH STRING RELEVANCE STRATEGY TO HELP USER EXPRESSION QUERIES

Nampalli Radhika[1]., P. Indira Nagavalli[2]., M. Sravanthi[3]., A. Geethika[4]., S. Meghana[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- radhika_ckv29@yahoo.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0568, 15RG1A05C6, 15RG1A0514, 15RG1A05K3),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— For the most important proposals applicable to the users' knowledge needs which are found near the database issuer site, we develop the first ever Location-aware keyword query Suggested Architecture. There is no way to think of user positions in current keyword advice approaches and even the outcomes of inquiries, i.e. users' spatial proximity to the results found is not taken as a factor in the recommendations. We inform you of a weighted keyword graph that shows both the semanticization of the keyword query and the spatial distance between the documents resulting and the user location. Our proposed LKS architecture is orthogonal with all recommendation approaches that use the question URL bipartite graph and could easily be integrated. LKS has a different objective and is thus different from other suggestion approaches for localization. The first problem in our LKS is how the keyword question similitudes can be calculated when spatial distance factor is reported. We performed tests with two denser models in our dense America-D datasets to ensure this statement. The hybrid method particularly outperforms other methods because in the ink propagation procedure it uses spatial and textual considerations, and thus better forecasts the flow and gradient propensity of the ink, achieves better divisions. To solve the problem, create a baseline formula from formula BCA. Then we proposed a partition-based algorithm that measures all of the candidate's partition level keyword questions and uses a lazy system to help minimise computing costs.

***Keywords*— Keyword Query suggestion, weighted-keyword, spatial databases, query-URL.**

1. INTRODUCTION

We recommend the very first Suggestion Application Location-aware keyword questionnaire. The benefit of LKS is shown. No current approaches include a keyword query recommendation for location-aware comprehension. An area-aware proposal is "lobster," which can find documents d4 and d5 in the vicinity which are also highly important to the original consumer quest. Unlike all prior methods that disregard positions, LKS sets the border weights of the KD-graph not just to catch the semantic significance between keyword queries [1]. Keyword search suggestions allow users to navigate the correct information without understanding how to articulate their questions accurately. There is no way to think of user positions in current keyword advice approaches and even the outcomes of inquiries, i.e. users' spatial proximity to the results found is not taken as a factor in the recommendations. Finally, Li et al. cluster queries from the search logs to derive query principles to pick recommended questions and to rehearse a probabilistic model with a greedy heuristic algorithm in order to achieve the diversification of recommendations.

Literature Survey: To the very best of our understanding, no previous work views user location in query suggestion. The vector of the query q includes the clicked URLs through the users who posed q as terms and also the weights are calculated according to term frequency and also the click recognition from the URL within the solutions [2]. Song and that he combine both clicked and skipped URLs from users within the query-URL bipartite graphs to be able to also consider rare query suggestions. Anagnostopoulos et al. formulate the query recommendation problem like a decision problem regarding how to perturb the transition odds between queries within the query-flow graph in order to increase the expected utility of the random walk. User session data are transformed into concept sequences and listed in a suffix tree. Cucerzan and White-colored generate query suggestions according to user squeeze pages. The aim would be to generalize an SQL query in situation of too couple of or no results. Bahmani et al. approximate PPR by counting the amount of occasions a node is visited by pre-computed random walks.

2. BASIC METHOD:

In Existing system after submitting a keyword query, the consumer might not be pleased with the outcomes, therefore the keyword suggestion module from the internet search engine recommends some m keyword queries that are likely to refine the user's search within the right direction. However, no existing methods provide location-aware keyword query suggestion (LKS), so that the recommended queries retrieve documents not just associated with the consumer information needs but additionally located close to the user location. This requirement emerges because of the recognition of spatial keyword search. Google processed a regular average of four.7 billion queries this year,1 a considerable fraction which have local intent and target spatial web objects or geo-documents. Disadvantages of existing system: However, the relevance of search engine results in lots of applications is proven to be correlated using their spatial closeness towards the query issuer.

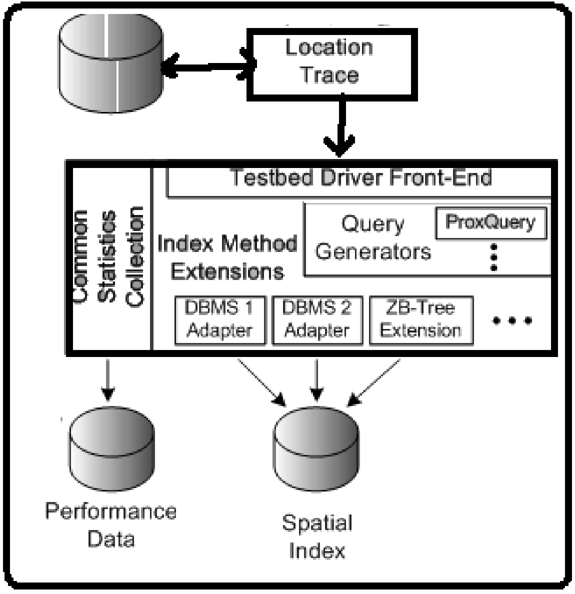


Fig.1.Proposed framework

3. ENHANCED QUERY SCHEME:

We advise the very first Location-aware Key phrase query Suggestion framework. We illustrate the advantage of LKS utilizing a toy example. Consider five geo-documents d1-d5 as listed. Each document is connected having a location [3]. Think that a person issues keyword query sea food at location q. Observe that the appropriate documents d1-d3 are not even close to q. An area-aware suggestion is "lobster", which could retrieve nearby documents d4 and d5 which are also highly relevant to the user's original search intention. However, the relevance of search engine results in lots of applications is proven to be correlated using their spatial closeness towards the query issuer. Within this paper, we design an area-aware keyword query suggestion framework. In compliance to previous query suggestion approaches LKS constructs and utilizes a keyword-document bipartite graph, which connects the keyword queries using their relevant documents. Benefits of suggested system: This LKS framework supplying keyword suggestions which are highly relevant to the consumer information needs and simultaneously can retrieve relevant documents close to the user location. Set up a baseline formula extended from formula BCA is brought to solve the issue. Then, we suggested a partition-based formula which computes the lots of the candidate keyword queries in the partition level and relies on a lazy mechanism to help reduce the computational cost. Empirical research is conducted to review the potency of our LKS framework and also the performance from the suggested algorithms. The end result implies that the framework can provide helpful suggestions which PA outperforms the baseline formula considerably.

Framework: two intuitive criteria for choosing good suggestions are: (i) the recommended keyword queries should fulfill the user's information needs according to kq and (ii) the recommended queries can retrieve relevant documents spatially. Performing keyword suggestion instantly is essential for that applicability of LKS used [4]. However, RWR search includes a high computational cost on large graphs. Previous focus on scaling up RWR search require pre-computation and/or graph segmentation. Set up a baseline formula extended from formula BCA is brought to solve the issue. Then, we suggested a partition-based formula which computes the lots of the candidate keyword queries in the partition level and relies on a lazy mechanism to help reduce the computational cost. Therefore, the direct relevance from a keyword query along with a clicked document is taken through the edge weight. In addition, the semantic relevance between two keyword queries is taken by their closeness within the graphG. Observe that this edge adjustment is query-dependent and dynamic. Without effort, the RWR score of the node v in graph Gq models the probability that the random surfer beginning from kq will achieve v.

Algorithms: Within our implementation, the load of every edge e is adjusted according to online, at that time once the source node of e is disbursing ink. The processing of the keyword query node involves retaining some of their active ink and disbursing some to the neighbor document nodes in line with the adjusted edge weights. Beginning with one unit of active ink injected into node kq, BA processes the nodes within the graph in climbing down order of the active ink. Not the same as typical personalized Page Rank problems. To enhance the performance of BA, within this section, we advise a partition-based formula that divides the keyword queries and also the documents within the KD-graph G into groups [5]. The priority queue utilized in BA maintains the nodes which will distribute ink, however the priority queue utilized in PA records the partitions that'll be processed. However, in formula PA, we adopt a lazy distribution mechanism that depends on threshold. Priority queue C stores the candidate suggestions in climbing down order of the retained ink, initialized as empty. The ranking of the keyword query node in C is updated and also the active ink AINK is modified. The potency of our LKS framework when compared with query suggestion that doesn't consider locations is evaluated. All tested methods were implemented using Java. Additionally, we cleaned the query log by taking out the keyword queries without click information with frequency. Just the phrases ending with whether noun or perhaps an adjective with frequency a minimum of 3 are stored, to be able to reduce the amount of noisy queries. LKS recommends towards the user alternative query keywords, which match the user’s intention and simultaneously find nearby documents. Thinking about the 2 criteria of excellent suggestions, we evaluate (i) the semantic relevance from the recommended keyword queries w.r.t. the user’s initial query and (ii) the amount of nearby documents retrieved through the query suggestions. To guarantee the fairness from the user study, the participants weren't accustomed to the facts of the project and also the particular b setup from the three scenarios. However, SD verifies effectiveness from the suggestion through the relevance from the retrieved nearby documents [6]. The queries recommended by INF can retrieve more nearby locations. Within this paper, we suggested an LKS framework supplying keyword suggestions which are highly relevant to the consumer information needs and simultaneously can retrieve relevant documents close to the user location. However, the amount of documents retrieved through the LKS-recommended queries is considerably greater compared to either the initial input, or even the INF recommended keyword queries. Following the direct look at recommended query keywords in the last experiment, we currently assess the nearby documents retrieved by them. Used, users only think about the highly rated suggestions. Formula PA outperforms BA for those values of b with a wide margin. PA runs fast for small values, that the approximation error is low. Empirical research is conducted to review the potency of our LKS framework and also the performance from the suggested algorithms. To ensure this assertion, we conducted experiments using two denser versions in our datasets the dense America online-D. Particularly, the hybrid method outperforms other approaches since it uses both spatial and textual factors throughout the ink propagation procedure, and therefore predicts better the way the ink may have a tendency to flow and cluster, achieving better partitioning [7]. To create our framework scalable, we advise a partition-based approach that outperforms the baseline formula by as much as a purchase of magnitude. The suitability in our framework and also the performance from the algorithms are evaluated using real data.

4. CONCLUSION:

Used, consumers just think about the highest regarded proposals. For certain values b with a wide spectrum, Formula PA exceeds BA. PA functions easily with small prices, which are poor. The final result means that the system will include useful advice that PA significantly surpasses the basic formula. We know that PA is a lot more stable for certain and significantly outperforms BA when a small one is. To solve the problem, create a baseline formula from formula BCA. Then we proposed a partition-based algorithm that measures all of the candidate's partition level keyword questions and uses a lazy system to help minimise computing costs. An area-aware proposal is "lobster," which can find documents d4 and d5 in the vicinity which are also highly important to the original consumer quest.

REFERENCES:

[1] Shuyao Qi, Dingming Wu, and Nikos Mamoulis, “Location Aware Keyword Query SuggestionBased on Document Proximity”,

ieee transactions on knowledge and data engineering, vol. 28, no. 1, january 2016.

[2] I. S. Dhillon, “Co-clustering documents and words using bipartite spectral graph partitioning,” in Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2001, pp. 269–274.

[3] K. Avrachenkov, N. Litvak, D. Nemirovsky, E. Smirnova, and M. Sokol, “Quick detection of top-k personalized PageRank lists,” in Proc. 8th Int. Workshop Algorithms Models Web Graph, 2011, vol. 6732, pp. 50–61.

[4] A. Anagnostopoulos, L. Becchetti, C. Castillo, and A. Gionis, “An optimization framework for query recommendation,” in Proc. ACM Int. Conf. Web Search Data Mining, 2010, pp. 161–170.

[5] D. Fogaras, B. R_acz, K. Csalog_any, and T. Sarl_os, “Towards scaling fully personalized PageRank: Algorithms, lower bounds, and experiments,” Internet Math., vol. 2, no. 3, pp. 333–358, 2005.

[6] H. Ma, H. Yang, I. King, and M. R. Lyu, “Learning latent semantic relations from clickthrough data for query suggestion,” in Proc. 17th ACM Conf. Inf. Knowl. Manage., 2008, pp. 709–718.

[7] U. Ozertem, O. Chapelle, P. Donmez, and E. Velipasaoglu, “Learning to suggest: A machine learning framework for ranking query suggestions,” in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2012, pp. 25–34.

A VERIFIABLE COMPLEX SYSTEM TO TEST AND ASSESS FUNCTIONAL CORRECTIONS

Sashirekha Tejavat[1]., S.Sai Priya [2]., Sravshiran mai [3] ., Thippani Sadhvika [4]., P. Apurva [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- shashirekha.tejavath@gmail.com)
2, 3, 4, 5 B.Tech IV Year CSE, (16RG1A0591, 16RG1A0589, 16RG1A0593, 15RG1A0580),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract*— Current research applies metamorphic testing to a quantifiable tool for the consistency of applications, not limited to software performance screening and validation. However, our user-oriented research methodology varies from previous user engineering orientation. We have done research on search engines as Google. Without talking to prospective algorithms or device requirements, we defined MRs from a user viewpoint. More broadly, it allows user to recognize that even without the full technical documentation, always the situation with web-based applications, poorly developed software and open source, a technique suited to their particular needs. Due to the potential absence of a target and the normally known oracle, the different engines are difficult to evaluate using traditional techniques. We looked at keyword-based and semantine search functionality in this analysis and we identified several helpful MRs and the appropriate consistency metrics. The above issues with the use of MT are solved and hence the usefulness of MT is newly demonstrated. Searching is certainly bad in a certain situation and requires some particular features, which are a very small group of all the Internet index engine functions..

***Keywords*— Quality assessment, oracle problem, lack of system specification, metamorphic testing, user-oriented testing**

1. INTRODUCTION

Almost any technique in software testing expects an oracle, a process by which testers can check the relation between test situations. To solve the oracle problem, the method of metamorphic testing (MT) continues to be developed. In this article, the above issues with MT are addressed and a new dimension of the efficacy of MT is seen. We have used our approach for evaluating various primary search engine software characteristics such as Google, except for purposes unrecognised and oracles normally recognized, under separate organizational profiles [1]. We provide a research solution that reduces the downside of authentication, evaluation and quality control by internet search engines. Search engines like Google for consumers are indicative of a wide range of tech products that are unregulated. The results are useful to developers and consumers of Internet search engines and our solution will efficiently mitigate the oracle dilemma and the complexities of checking, validating and testing massive, high quality information systems in relation to excessive requirements. When creating software programmes and components, the developer has to worry of these aspects and also has to choose a formula / specification by various candidates as all models have their own advantages and constraints. You should describe MRs as the attributes required for the things that a successful search engine will want you to have, in order to meet your particular needs, irrespective of the way the Internet search engine was developed. Our methodology can also be extended outside verification and validation for product quality evaluation. The consumer also can access the implemented source code. MT was initially suggested like a verification technique, where an MR is really a necessary property from the formula to become implemented. Zhou et al. conducted pilot studies to check the running correctness of keyword-based search of Google, Yahoo! and Live Search. Imielinski and Signorini basically also used the logical consistency relationships to check “how semantic” an internet search engine is [2]. Our user-oriented testing approach, however, differs from previous focus on finish-user software engineering. More lately, MT techniques are also unconditionally accustomed to identify internet search engine censorship. Within this study, we considered both keyword-based and semantic search features, and identified numerous helpful MRs and corresponding quality metrics.

2. CLASSIC METHOD:

MT doesn't concentrate on the verification of every individual output, but rather checks the relationships one of the inputs and outputs of multiple executions from the program under test. The current research extends metamorphic testing right into a quantifiable method for software quality assessment, including, however is not restricted to, the verification and validation of software correctness [3]. Disadvantages of existing system: It's imperative that search engines like Google supply the preferred result based on the queries joined. It's, however, very hard to assess some key characteristics of the various search engines. For example, because of the sheer amount of data on the web, it's very hard to verify or validate the correctness from the software systems in order to assess the precision and completeness from the search engine results. Also, because of the apparent subjectivity of various idol judges, objective assessment of Google listing relevance and ranking quality is extremely difficult.

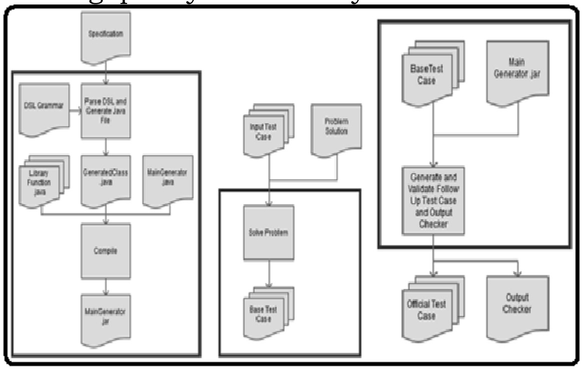


Fig.1.Block diagram of proposed system

3. QUALITY APPROACH:

We applied our approach to relieve the oracle problem for that testing and quality assessment of (web) search engines like Google. Search engines like Google are software systems designed to look for info on the internet, and therefore are the primary interface by which people uncover information on the web searching is among the most widely used functionalities from the Internet, second simply to email. This paper addresses the above mentioned problems using MT, and consequentially demonstrates new size of the effectiveness of MT. For any given internet search engine, its quality of search could be considerably different for various query languages, various kinds of query words, and various domains being looked. This finding supplies a hint for those developers to recognize the force and weakness of the systems, and it is helpful for those users to select an appropriate internet search engine in order to better construct their queries [4]. A number of empirical research has been conducted to check the program characteristics of 4 major search engines like Google, namely, Google, Bing, Chinese Bing, and Baidu. Within this paper, we present a testing approach that alleviates the down sides in internet search engine verification, validation, and quality assessment. Benefits of suggested system: Therefore, the consumer does not need to comprehend the machine in the whole to be able to validate the internet search engine rather, he/she only requires a testing technique that informs him/her set up couple of functions directly active in the search delivers what he/she would like. Once the test fails, it may either indicate a fault within the implemented software system or perhaps a deficiency within the formula(s) selected through the internet search engine developer-for validation purposes, the consumer doesn't need to separate both of these cases. Most multiple-comparison results also were built with a record and practical significance, indicating our approach works well. We've also discussed the investigated software characteristics within the framework from the software quality model standard ISO/IEC 25010.

Implementation Methods: Looking engine's responses for that source and follow-up test cases will be compared against predefined logical consistency relationships. For a lot of search engines like Google including individuals investigated in our paper, when the test is not enclosed by double speech marks, synonyms is going to be employed instantly. To check searching engine's information retrieval capacity in situations where synonyms can be utilized for semantic search, a great technique is to create an evaluation query q that best characterizes a target web site p. MPTitle is yet another "No Missing web Page" group MR. Even though the MPSite MR always uses speech marks for exact searching, MPTitle involves both exact and inexact query terms [5]. Based on Google specs, Google searches "anywhere within the document. To determine the similarity of these two result sets, we make use of the metric Jaccard similarity coefficient. Its design was inspired with an internet search engine assessment technique informally utilized in industry, which is dependent on the explanation that the good internet search engine should return similar recent results for similar queries. The 2nd number of MRs is known as "Consistent Ranking." Its first MR is SwapJD, which assesses looking engines' ranking stability in line with the indisputable fact that a reliable internet search engine should return similar recent results for similar queries. The Web is dynamic and internet search engine databases could be updated instantly, which can lead to inconsistencies between your source and follow-up responses. Search engines like Google aren't the same as conventional database applications for the reason that they frequently return approximate instead of exact results. It will be noted, however, the internet search engine failure might not always result from a programming fault. A number of experiments specified for reliability assessment using MPSite, where two kinds of queries were issued, namely, British queries and Chinese queries, once we desired to begin to see the impact from the operational profile on reliability. MPTitle was created in the outlook during user validation instead of for correctness verification or failure recognition. An internet search engine may return spun sentences for queries that differ in word order, particularly when an order is essential, potentially altering this is from the query. To reduce the outcome of word order on query meanings, only names were utilized as fundamental query products for MPReverseJD [6]. We further designed three usage patterns: the very first pattern uses people’s names only, the 2nd pattern uses company names only, and also the third pattern uses drug names only. In the outlook during consumer experience and validation, you is going to be unhappy to get 3 results should there be really a minimum of 28 WebPages that contains all the words. It will be noted that the style of SwapJD differs from those of MPReverseJD. To identify military services weapons web site, MPReverseJD uses rigorous measures to boost precision and exactness. SwapJD was created in the outlook during understanding internet search engine behavior having a concentrate on its stability for semantically similar queries. When searching the net, there's a phenomenon referred to as users’ domain bias, where users have a tendency to click “top domains” inside a SERP. The .com domain was initially meant for commercial use, but it is typically the most popular top-level domain, and it is utilized by all kinds of entities. We made the decision, therefore, to check out the very best 50 recent results for the follow-up query: When the first rated result for that source query A doesn't appear one of the top 50 recent results for the follow-up query B then an anomaly is going to be recorded. The query language includes a strong effect on the performance: Google British and Bing British ongoing to outshine Google Chinese and Bing Chinese, correspondingly. With regards to validation, random sampling of test cases carrying out a usage-profile-based probability distribution is frequently preferred. Our random sampling strategy, which doesn't refer somewhere logs, is a straightforward means to fix the above mentioned problems and offers a typical ground for fair comparison of various systems. For MPSite and MPTitle, a resource totally an expression enclosed by double speech marks- this type of phrase is significant because, first, it includes valid British or Chinese words and, second, the style of the experiments guarantees the source response always contains a number of results, meaning the saying belongs to some web documents and it is hence significant [7]. Metamorphic testing was suggested like a verification technique, where metamorphic relations were recognized by talking about the prospective formula to become implemented. Within this paper, we've shown the practicality of MT as being a unified framework for software verification, validation, and quality assessment.

4. CONCLUSION:

The queries that create a mistake can be seen as a kind of "hard query" that returns from a search engine are not good in their calibre. A variety of stakeholders, such as app creators, operators, consumers, etc., are considered. Nevertheless, developers should be mindful of knowledge on adopted algorithms, and this is why MR's can be identified, implemented by those MRs checked, and the principal explanation for any detected faults discovered. The statistically important findings with high effect size values were returned from all ANova Analysis. The analytical findings prove that we support developers and consumers with our approach. First, we can recognise various forms of failures efficiently. Secondly, we find that organizational profiles have a major impact on the search calibre. Metamorphic checks are a validation tool, in which you can verify that the programmed works well even without the right oracle. This expands metamorphic testing to a tech, validation and quality management user-oriented process, and carries out huge observational studies on four main online search engines such as Google, Bing, Chinese Bing, and Baidu. Instant errors and abnormalities to be identified with MRs could provide hints for the establishment, which is the next research area, of the runtime self-correction mechanisms.

REFERENCES:

[1] ZhiQuan Zhou, Shaowen Xiang, and TsongYueh Chen, “Metamorphic Testing for Software QualityAssessment: A Study of Search Engines”, ieee transactions on software engineering, vol. 42, no. 3, march 2016.

[2] A. J. Ko, R. Abraham, L. Beckwith, A. Blackwell, M. Burnett, M. Erwig, C. Scaffidi, J. Lawrance, H. Lieberman, B. Myers, M. B. Rosson, G. Rothermel, M. Shaw, and S. Wiedenbeck, “The state of the art in end-user software engineering,” ACM Comput. Surveys, vol. 43, no. 3, pp. 21:1–21:44, 2011.

[3] J. Zhang, J. Chen, D. Hao, Y. Xiong, B. Xie, L. Zhang, and H. Mei, “Search-based inference of polynomial metamorphic relations,” in Proc. 29th IEEE/ACM Int. Conf. Autom. Softw. Eng., 2014, pp. 701–712.

[4] J. R. Smarr, “Categorization by character-level models: Exploiting the sound symbolism of proper names,” Master’s thesis, The Symbolic Systems Program, Stanford Univ., Stanford, CA, USA, 2003

[5] J. Guo, G. Xu, X. Cheng, and H. Li, “Named entity recognition in query,” in Proc. 32nd Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2009, pp. 267–274.

[6] H. Liu, F.-C. Kuo, D. Towey, and T. Y. Chen, “How effectively does metamorphic testing alleviate the oracle problem?” IEEE Trans. Softw. Eng., vol. 40, no. 1, pp. 4–22, Jan. 2014.

[7] T. R. Levine and C. R. Hullett, “Eta squared, partial eta squared, and misreporting of effect size in communication research,” Human Commun. Res., vol. 28, no. 4, pp. 612–625, 2002.

A VIBRANT PLAN TO SENSE ADAPTED AND ANOMALOUS BEHAVIORS OF INTERNET USERS

Ambadi Vijetha[1]., V.G. Anupa[2]., V. Sai Snehitha[3]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda.,
Medchal., TS, India (✉:- vijethaambadi01@gmail.com)
2, 3 B.Tech IV Year CSE, (16RG1A05A2, 16RG1A05A1),
Malla Reddy College of Engineering for Women, Maisammaguda., Medchal., TS, India.

Abstract— This groundbreaking mining problem can be solved by means of three phases: preprocedure for the extraction of probabilistic issues and sessions for different users, the generation of (expected) STP candidates with support values by pattern-growth for each user, decision making on URSTPs by looking for user-conscious rarities analysis of derived STPs. Poor deterministic information is available, a comprehensive survey. The help of the idea is easily the most common metric for assessing the regularity of the pattern and it is known to be the number or percentage of sequences containing the pattern in the target database. The patterns obtained are not often interesting since the unusual but relevant patterns reflecting personalized and irregular behavior, due to low funding, are pruned. We suggest a framework to solve this problem pragmatically and to use suitable algorithms. Initially, we include preprocessing with heuristic methods of extraction and recognition of topic topics. This strategy can be viewed as a change between the objects purchased by the STP and the probabilistic subjects inside the documents purchased during the relevant session. The results show that our strategy will definitely catch and articulate online users' individual behaviors.

Keywords— Web mining, sequential patterns, document streams, rare events, pattern-growth, dynamic programming.

1. INTRODUCTION

We advise Consecutive Subject Patterns (STPs) and develop the problem of mining user-compliant Rare Consecutive Theme Patterns on Web streams to recognize and defect the customized and pathological behavior of online users. We would also develop user-conscious steps to address diverse needs Improve the accuracy of parallel algorithms primarily in the mining sector, and emphasis on real-time text transmission-driven algorithms. We also aim to describe complex event models according to STPs, for example by placing timing restrictions on subsequent problems, and corresponding effective mining algorithms in style [1]. The web-produced and circulated textual documents still change in a number of ways. They are generally uncommon but more common for specific users, as is the case with many real-life situations, such as in real-time surveillance of irregular user activity. The majority of existing works are dedicated to subject modeling and also the evolution of person topics, while consecutive relations of topics in successive documents printed with a specific user are overlooked. We're also thinking about the twin problem, i.e., finding STPs occurring frequently overall, but relatively rare for particular users. In addition to this, we'll develop some practical tools legitimate existence tasks of user behavior analysis on the web. To be able to characterize user behaviors in printed document streams, we study the correlations among topics obtained from these documents, particularly the consecutive relations, and specify them as Consecutive Subject Patterns (STPs). For any document stream, some STPs can happen frequently and therefore reflect common behaviors of involved users. STPs can characterize complete browsing behaviors of readers, so when compared with record methods, mining URSTPs can better uncover special interests and browsing habits of Online users, and it is thus competent to give effective and context aware recommendation on their behalf [2]. A preprocessing phase is essential and essential to get abstract and probabilistic descriptions of documents by subject extraction, after which to acknowledge complete and repeated activities of Online users by session identification. In lots of real applications, document collections generally carry temporal information and may thus be looked at as document streams. We advise a framework to pragmatically solve this issue, and style corresponding algorithms to aid it. Within the facet of consecutive patterns for topics, Hariri et al. presented a strategy for context-aware music recommendation according to consecutive relations of latent topics. The preprocessing strategies including subject extraction and session identification are presented at length, where several heuristic methods are discussed For uncertain data, the majority of existing works studied frequent itemset mining in probabilistic databases. STPs happen so that you can combine a number of inter-correlated messages, and may thus capture such behaviors and connected users.

2. BASIC SYSTEM DESIGN:

The majority of existing works examined the evolution of person topics to identify and predict social occasions in addition to user behaviors. Many mining algorithms happen to be suggested according to support, for example Prefix Span, Free Span and SPADE. They found frequent consecutive patterns whose support values aren't under a person-defined threshold, and were extended by SLPMiner to cope with length decreasing support constraints [3]. Muzammal et al. centered on sequence-level uncertainty in consecutive databases, and suggested techniques to assess the frequency of the consecutive pattern according to expected support, within the frame of candidate generate-and-test or pattern-growth. Disadvantages of existing system: The acquired patterns aren't always interesting for the purpose, because individual's rare but significant patterns representing personalized and abnormal behaviors are pruned because of low supports. In addition, the algorithms on deterministic databases isn't relevant for document streams, because they unsuccessful to handle uncertainty in topics.

3. VIBRANT ENHANCEMENT:

To be able to characterize user behaviors in printed document streams, we study the correlations among topics obtained from these documents, particularly the consecutive relations, and specify them as Consecutive Subject Patterns (STPs). To resolve the innovative and serious problem of mining URSTPs in document streams, many new technical challenges are elevated and will also be tackled within this paper. First of all, the input from the task is really a textual stream, so existing techniques of consecutive pattern mining for probabilistic databases can't be directly put on solve this issue [4]. A preprocessing phase is essential and essential to get abstract and probabilistic descriptions of documents by subject extraction, after which to acknowledge complete and repeated activities of online users by session identification. Next, cellular the actual-time needs in lots of applications, both precision and also the efficiency of mining algorithms are essential and really should be taken into consideration, specifically for the probability computation process. Thirdly, not the same as frequent patterns, the consumer-aware rare pattern concerned this is a new idea along with a formal qualifying criterion should be well defined, in order that it can effectively characterize the majority of personalized and abnormal behaviors of Online users, and may adjust to different application scenarios. And correspondingly, without supervision mining algorithms for these sort of rare patterns have to be developed in a way not the same as existing frequent pattern mining algorithms. Benefits of suggested system: We advise a framework to pragmatically solve this issue, and style corresponding algorithms to aid it. Initially, we give preprocessing procedures with heuristic means of subject extraction and session identification. Then, borrowing the minds of pattern-development in uncertain atmosphere, two alternative algorithms are made to uncover all of the STP candidates with support values for every user. That gives a trade-off between precision and efficiency. Finally, we present a person-aware rarity analysis formula based on the formally defined qualifying criterion to choose URSTPs and connected users. We validate our approach by performing experiments on real and artificial datasets [5].

The URSTP: The majority of existing creates consecutive pattern mining centered on frequent patterns, however for STPs; many infrequent ones will also be intriguing and ought to be discovered. Once the session group of a subject-level document stream is acquired, we are able to have some concrete cases of an STP for every session. Because this paper puts forward a cutting-edge research direction on Web data mining, much work could be built onto it later on. Initially, the issue and also the approach may also be used in other fields and types of conditions. Specifically for browsed document streams, we are able to regard readers of documents as personalized users making context-aware recommendation on their behalf. This method could be considered as sequence matching between your purchased topics specified by the STP and also the probabilistic topics occurring within the purchased documents owned by a particular session. Furthermore, additionally they centered on frequent patterns and therefore can't be employed to uncover rare but interesting patterns connected with special users. we advise a singular method of mining URSTPs in document streams. It includes three phases. Initially, textual documents are crawled from some micro-blogs or forums, and constitute a document stream because the input in our approach. After preprocessing, we have some user-session pairs. For every document, the generated subject proportion could have some topics with low probability. Two classical time-oriented heuristic methods does apply here, because both versions is dependent on an acceptable assumption: Time Interval Heuristics and Time Period Heuristics. Beyond that, some websites allow users to construct hyperlinks among printed documents, so within this situation, you'll be able to find better and user-specific partitions if users really produce these links to point complete behaviors. to be able to enhance the efficiency in our approach, we give an approximation formula to estimate the support values for those STPs [6]. Both algorithms are made in the way of pattern-growth. It formulates a brand new type of complex event patterns according to document topics, and it has wide potential application scenarios, for example real-time monitoring on abnormal behaviors of Online users. Within this paper, several new concepts and also the mining problem are formally defined, and several algorithms are made and combined to systematically solve this issue. Hence, even when an STP has several instances inside a session, we are able to pick the one using the largest probability because the representative occurrence from the STP within the session. In the end the STP candidates for those users are discovered, we'll result in the user-aware rarity analysis to choose URSTPs, which imply personalized, abnormal, and therefore significant behaviors. Because the problem of mining URSTPs in document streams suggested within this paper is innovative, there aren't any other complete and comparable methods for this because the baseline, but the potency of our approach in finding personalized and abnormal behaviors. Within the preprocessing phase, we make use of a public package from the Twitter-LDA model. it's very hard to get the exact ground truth of those users for that at random crawled datasets. Here, we create a reasonable assumption that “verified” users in Twitter are more inclined to have particular and repeated behaviors than ordinary users [7]. Furthermore, the main difference caused through the two subject models for URSTP mining is a lot smaller sized than that for straightforward subject mining. An acceptable explanation would be that the user regards his team like a family, so frequently quotes some existence philosophy to inspire his teammates and harmonize they atmosphere. We are able to reckon that the previous is really a news reporter who always publishes official broadcasts adopted by the development of players, however the latter is simply a regular fan who forwards some broadcast messages after commenting on players because the first reaction.

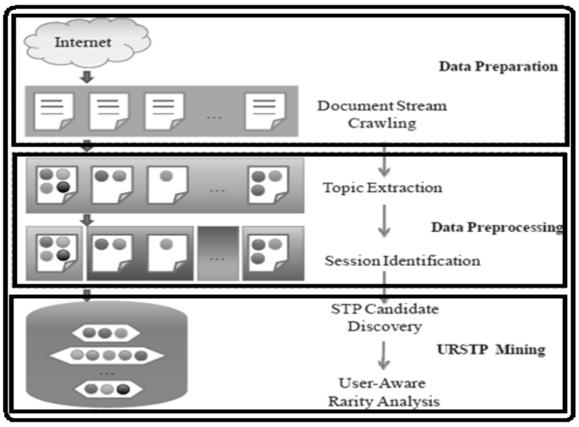


Fig.1.Proposed framework

4. CONCLUSION:

But even for our URSTP mining, the qualification criteria include both global sponsorship of the STP and also the relative rarity from the STP for any local user. In any design-growing phase for each particular user we can only receive local support in sessions linked to the user, but not global support for all sessions, thus whether the current STP is indeed a URSTP cannot be determined. It is a substantial and difficult issue to delete URSTPs in written web streams of documents. To our best understanding, this is indeed the first work which, in addition to its rare steps, provides formal descriptions of STPs and highlights the question of URSTP mine in document streams such that customized and irregular behaviors can be characterized and identified for online users. In addition to interesting and interpretable URSTPs on on-line feeds, which could catch the customized and irregular habits and features of users, tests carried out in actual (Twitter) and artificial data systems demonstrate the suggested solution very efficiently and effectively. In this article, we notice the similarities between subsequent documents printed within one document stream by the same person. The findings suggest that our methodology will definitely capture and articulate web users' individual behaviors.

REFERENCES:

[1] Jiaqi Zhu, Member, IEEE, Kaijun Wang, Yunkun Wu, Zhongyi Hu, and Hongan Wang, Member, IEEE, “Mining User-Aware Rare Sequential TopicPatterns in Document

Streams", IEEE Transactions on Knowledge and Data Engineering, 2016.

[2] M. Spiliopoulou, B. Mobasher, B. Berendt, and M. Nakagawa, "A framework for the evaluation of session reconstruction heuristics in web-usage analysis," INFORMS J. Comput., vol. 15, no. 2, pp. 171–190, 2003.

[3] K. Chen, L. Luesukprasert, and S. T. Chou, "Hot topic extraction based on timeline analysis and multidimensional sentence modeling," IEEE Trans. Knowl. Data Eng., vol. 19, no. 8, pp. 1016–1025, 2007.

[4] W. Li and A. McCallum, "Pachinko allocation: DAG-structured mixture models of topic correlations," in Proc. ACM ICML'06, vol. 148, 2006, pp. 577–584.

[5] J. Pei, J. Han, B. Mortazavi-Asl, H. Pinto, Q. Chen, U. Dayal, and M. Hsu, "PrefixSpan: Mining sequential patterns by prefixprojected growth," in Proc. IEEE ICDE'01, 2001, pp. 215–224.

[6] Z. Zhang, Q. Li, and D. Zeng, "Mining evolutionary topic patterns in community question answering systems," IEEE Trans. Syst., Man, Cybern. A, vol. 41, no. 5, pp. 828–833, 2011.

[7] T. Bernecker, H.-P. Kriegel, M. Renz, F. Verhein, and A. Zuefle, "Probabilistic frequent itemset mining in uncertain databases," in Proc. ACM SIGKDD'09, 2009, pp. 119–128.

BEHAVIORAL MODELING OF MULTI MASTER I2C BUS CONTROLLER WITH XILINX VERILOG HDL SIMULATION

Ch. Mahesh[1]., G. Punvitha [2]., K. Krishnapriya [3]., K. Pushpa [4]., K. Manisha [5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ : chekuri20@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0445 , 15RG1A0451, 15RG1A0452, 15RG1A0461), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— This article describes the design and implementation of a multi-master integrated circuit bus controller (often written as or IIC). The multi-master C interface bus is a circuit for performing serial communication based on data format transfer. The loss of the arbitration recognition function enables communication with multiple teachers. Communication takes place in four data transmission modes, depending on the application. The module was developed in Verilog HDL. It is simulated and synthesized with Xilinx Design Suite 13.2

Keywords— C, Master, Serial data communication, Slave, Xilinx.

1. INTRODUCTION

In serial data communication, there are many protocols such as RS-232, RS-422, RS-485, SPI (serial interface device), and micro cables for connecting high and low speed devices. These protocols require more IC (integrated circuit) pin connections for you to perform serial data communication, and as the physical size of the IC has decreased over the years, we need less pin connection to perform serial data communication. USB / SPI / Micro Cable Most UARTs are point-to-point data bus transmission systems. They use techniques such as data route multiplexing and message forwarding to provide services to multiple devices. To solve this problem, Phillips introduced the C protocol. This protocol requires two lines to communicate with two or more chips and can control one network chip from devices that typically have two end I / O pins. Other bus protocols require more pins and signals to connect devices.

2. LITERATURE REVIEW

Bollam Eswari et al. [1] discussed the implementation of the C-FPGA protocol as the master C controller transfers data to and from the slave. All low-speed devices can be connected to each other through the C-Master controller. JJPatel and at. [2], They discussed the design and implementation of the C-bus controller using Verilog, give an idea of the design of the C-bus controller, which is in the start / stop control, compared to the arbitration unit, the interface to the microprocessor, state machine, interrupt controller, clock generator and synchronizer. PKMehto and. In the [3] discussed about the design and implementation to connect two integrated devices.

II.C BUS SPECIFICATIONS

The Controller C-Bus is a bidirectional two-wire serial bus that provides a simple and efficient method of transferring data over short distances between many devices. C provides good support for communicating with various slowly integrated peripheral devices that are intermittently accessed because the hardware resource requirements are extremely small. It has the advantages of a simple protocol, low bandwidth, and short distance. It is easy to use to connect multiple devices and has a constructed address. The two C signals are serial data (SDA) and serial clock (SCL), as shown in Figure 1. The device that initiates a transaction on the C-Bus is called the master. The master usually controls the clock signal and the device that the master is pointing at is called the slave.

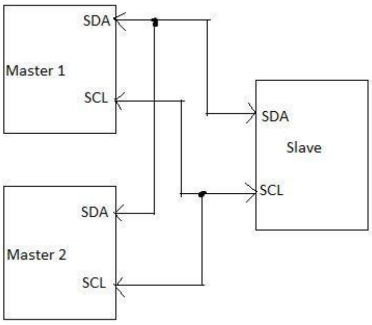


Figure 1: Multi-Master C devices

The C protocol supports multiple teachers, although most system designs include only one teacher. There can be one or more slaves on the bus. Teachers and slaves can receive data bytes and also transmit data bytes.

3. PROPOSED WORK

A. Data transfer

The SDA and SCL lines are two bidirectional lines. These are connected to a positive voltage supply via a pull-up resistor. The bus is free when both lines are "high". Data on the DID line is only valid when the SCL line is "high". It enables data exchange if the SCL line "fails". During the data transfer, the master generates the switch-on and switch-off conditions, which are unique conditions.

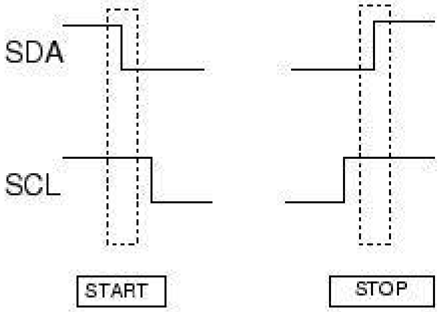


Figure 2: Start and stop conditions of the C-bus

The data on the SDA line must be stable during the HIGH period of the clock. A data line change is only permitted if the clock signal on the SCL line is LOW. It's as shown in Figure 3.

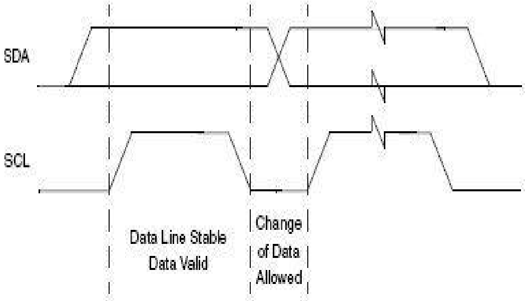


Figure 3: Data validity

B. Byte format

Each byte placed in the SDA line must be 8 bits long. There is no limit to the number of bytes that can be transferred through the transmission. A confirmation bit must follow each byte. The byte transfer takes place as shown in Figure 4.

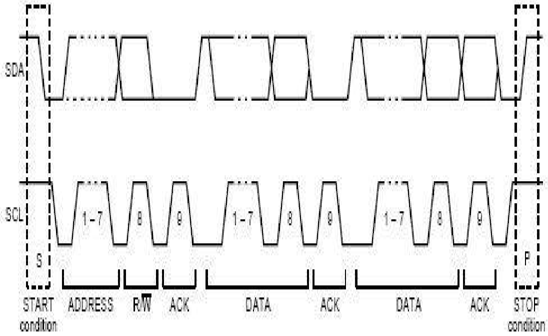


Figure 4: Byte transfer

For each transmission byte on the I²C bus and no longer a slave or data direction, provided that it sends a first MSB and LSB at the end. The format of the byte is shown in Figure 5.

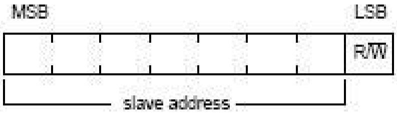


Figure 5: Byte format

C. Recognize

The clock associated with the detection is generated by the master. The receiver must leave the SDA line during the detection clock pulse. For this reason, LOW remains stable during the ALTO period of this clock pulse. The detection on the I²C bus is shown in Figure 6.

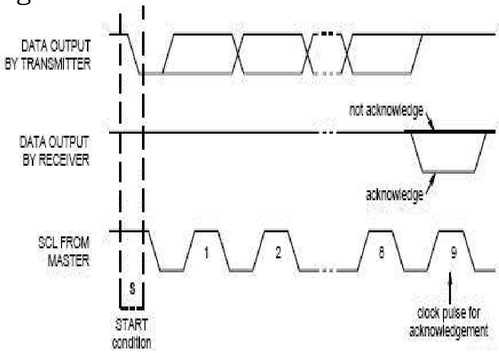
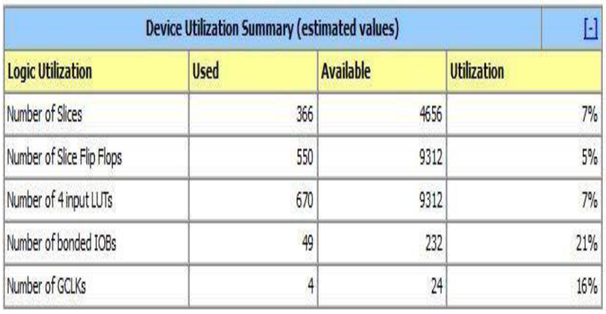


Figure 6: Detection in the C-Bus

5. ANALYSIS OF THE RESULTS

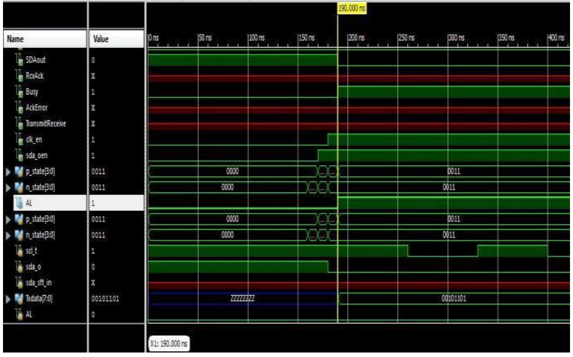
The I²C bus controller was developed in Verilog and receives the results of the simulation. The summary of device usage is shown in Table 1 below.



Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slices	366	4656	7%
Number of Slice Flip Flops	550	9312	5%
Number of 4 input LUTs	670	9312	7%
Number of bonded IOBs	49	232	21%
Number of GCLKs	4	24	16%

Table 1: Summary of device usage

The simulated result is as shown in Figure 10 and the view of RTL is as shown in Figure 11



Name	Value
SDAout	0
RcvAck	X
Busy	1
AckError	X
TransmitReceive	X
clk_en	1
sda_oen	1
p_state[3:0]	0011
n_state[3:0]	0011
AL	1
p_state[3:0]	0011
n_state[3:0]	0011
scl_t	1
sda_o	0
sda_sft_in	X
Txdata[7:0]	00101101
AL	0

Fig 7: Simulation waveform for multi-master I²C bus controller

4.CONCLUSION AND FUTURE SCOPE

The I²C master controller was implemented, simulated and synthesized for four operating modes. The designed controller is ideal for on-board applications. The controller can be used for integrated microprocessor boards, multiple low power applications, communications systems, and various automotive systems that are reliable and inexpensive.

High-speed mode devices are still fully compatible with devices ranging from as fast or standard (F / S mode) to bidirectional communication over a mixed-speed system bus. It also shows that the efficiency is better at high speed compared to all operating modes. However, depending on requirements, new devices can have an I²C bus interface in high-speed or high-speed mode

They prefer high-speed mode devices that can be designed for a larger number of applications.

The design of the C master controller has good applications in the near future, and the number of devices connected to a given system will increase day by day. Therefore, there is always a need for a system that supports multiple protocols. In all of these situations, the master controller C acts as an excellent support and will be essential for future design to support multiple parallel functions.

REFERENCES

1. P.K.Mehto, P.Mishra and S.Lal, " Design and Implementation for interfacing two integrated device using I2C bus", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, March 2013, pp. 3423-3426.
2. J.K.Singh, M.Tiwari, V.Sharma, "Design and Implementation of I2C Master Controller on FPGA using VHDL", International Journal of Engineering and Technology (IJET), Vol. 4, 2012, pp. 162 -166.
3. J.J.Patel, Prof B. H. Soni, "Design and Implementation of I2C Bus Controller using Verilog", Journal of Information, Knowledge and Research in Communication Engineering, Vol. 2, pp. 520 – 522.
4. M. Alassir, J. Denoulet, O. Romain & P. Garda, " A SystemC AMS Model of an I2C Master Bus Controller", International Conference,2006, pp. 154 – 158.
5. Bollam Eswari, N.Ponmagal, K.Preethi, S. G. Sreejeesh, "Implementation of I2C Master Controller on FPGA", International conference on Communication and Signal Processing, April 3-5, 2013, pp.1113-1116.

AUTOMATION SYSTEM FOR PARALYZED PEOPLE USING ANN BASED VOICE RECOGNITION FOR MEDICAL APPLICATIONS

Dr. Archek praveen kumar[1]., D.Swetha [2]., D.Swetha [3]., D.Sushmitha [4]., D.Vinitha [5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ : archekpraveen@yahoo.co.in)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0428 , 15RG1A0429, 15RG1A0430, 15RG1A0431), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— ***Voice is the most effective form of communication between people. This form of communication can also be a useful interface for interacting with machines. Therefore, the dependence on the speech recognition system has increased dramatically in recent years. There are different speech recognition methods like the Hidden Markov Model (HMM), the Hybrid Hidden Markov Model (ANN), etc. This article introduces the prototype of a speech recognition-based automation system for people with physical disabilities who suffer from quadriplegia or paraplegia (who cannot move body parts but can speak and hear) to control various devices and move the bed with only Voice control commands. According to your wishes and your comfort. The proposed model has a speech recognition model, an Arduino Uno microcontroller, a relay circuit for LED & buzzer and an adjustable bed motor. The speech recognition model must first be trained and the data must be saved before it can be used to recognize commands. As soon as the voice command is recognized, the Arduino controls the respected load via the relay circuit***

Keywords— ***Voice Recognition, ANN, Automation System for Paralyzed People, Arduino Uno, Motor, Buzzer, LED.***

1. INTRODUCTION

The voice is the most effective and natural way of communicating. People also want a similar, natural, simple and efficient way of communicating with machines. As a result, they prefer speech as a means of interacting with devices rather than another hectic surface like a mouse and keyboard. However, the voice is a complex phenomenon because the tone and human voice articulators as biological organs are not under our control and are not the same every time. Speech recognition or automatic speech recognition (ASR) plays an important role in human-machine interaction. Speech recognition uses a different method to recognize the word and to convert the speech signals into a sequence of words using an algorithm implemented in the form of a computer program. Various techniques are used for this process, such as: B. LPC, MFCC and ANN. Speech recognition systems are able to understand different languages and different words in a functional environment. The speech signal provides two important types of information: [1] speech content and [2] speaker identity. The speech recognition automation system can be used for various applications. [1] Can be used for home automation. [2] Can be used to control various devices for paralyzed patients. [3] It also has many uses such as phone book support, automatic language translation into foreign languages.

2. VOICE RECOGNITION PROCESS

The process of speech recognition is a complex and hectic task. Figure 1 shows the next steps in the speech recognition process.

2.1 Speech capture

The voice is the most effective form of human communication. The speaker's voice is received in the form of a wave. There is a large amount of software available that can be used to record the human voice. We save the voice signal in it in the form of ".mat". The acoustic atmosphere and receiving equipment can have a significant impact on the voice generated. At some point we have background noise or ambient reverberation with the speech signal that is undesirable and should not be processed further.

2.2 Speech pre-processing

In this step, the pre-processing block plays an important role in removing the unwanted signal. Finally, it improves the accuracy of speech recognition. Speech pre-processing typically includes noise filtering, signal smoothing, point-to-point detection, signal frames, signal windows, and echo cancellation and suppression. Only the original data was still processed.

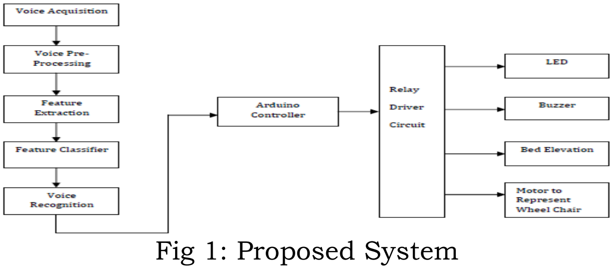


Fig 1: Proposed System

2.3 Extraction of Features

As we know, the voice differs from person to person. This is because each person has a different vocal cord that sounds different. In theory, it is possible to recognize the voice from the digitized waveform. However, due to the large variation in the speech signal, it is necessary to perform feature extraction in order to reduce these variations and the unwanted signal. Various technologies are available for feature extraction: These technologies are also useful in other areas of speech processing.

2.4 Classification of Features

The most common techniques for classifying features are described below. This type of system has complex mathematical functions and extracts hidden information from the input signal. HMM is the most widely used pattern recognition technology for speech recognition. HMM is a mathematical model given in the Markov model with an output distribution theorem? The HMM method divides the voice into smaller audible parts, and these parts represent the state in the Hidden Markov Model. And depending on the probability of transmission, there is a transmission from one state to another.

3. IMPLEMENTATION OF THE SOFTWARE

To design the system, we wrote code in MATLAB.

MATLAB is a high-level programming language of the fourth generation and offers an interactive environment for numerical calculation, visualization and programming.

Offers matrix manipulation; Plot functions and data; Implementation of various algorithms; Creation of user interfaces; provides an interface to programs written in other languages including C, C ++, Java, and FORTRAN. Analyze the data; develops algorithms; and build the necessary models and applications.

It has many built-in commands and math functions to aid the user in math calculations and making graphs. It is also used to perform numerical methods.

4. EQUIPMENT USED

The hardware implementation of the proposed system is explained below.45.1 Microphone and speech recognition module

The microphone that is used to capture the speech signal and send it to the speech recognition model is basically a collar microphone with a 3.5mm connector. In this system we used the Elechouse v3 speech recognition module for the speech recognition process shown in the figure below. The speech recognition module needs to be trained first, then it can be used to actually recognize the voice commands. Vote for the speaker. The speech input from the microphone is passed on to the speech recognition model, and here the input voice is compared with the previously stored trained speech commands. If it matches the stored and trained data, the control action takes place. In the circuit command. The speech recognition model v3 can store up to 80 commands of 1400 to 1500 ms each in its library, and out of 80 commands only 7 commands in the recognition module can be used for the recognition process. Therefore , only 7 controls are currently active. To add the following 7 commands you need to delete the detection module first. The model you selected has two ways to control the serial port: general input pins and general output pins. It has a detection accuracy of 99% under suitable conditions.

4.2 Arduino Uno microcontroller

The microcontroller we are using for the proposed model is shown in Figure 5. The Arduino microcontroller provides students and professionals with an affordable and affordable platform to create devices that interact with different types of sensors and actuators with a respectable environment. The Arduino microcontroller has an integrated development environment (IDE) that can be easily run on a PC and allows the user to write programs for the microcontroller in C or C ++ language, which is easy compared to other languages and is robust. The Arduino microcontroller board is based on the AT mega 328. The characteristics of the Arduino microcontroller are listed below. It has 14 digital input / output pins (of these 14 pins, all 6 can be used as PWM outputs) and 6 are used for analog inputs.

5. TEST RESULTS

Below we show the result of the test where the buzzer turns on and off every second. The following picture shows the configuration of our module and Arduino.

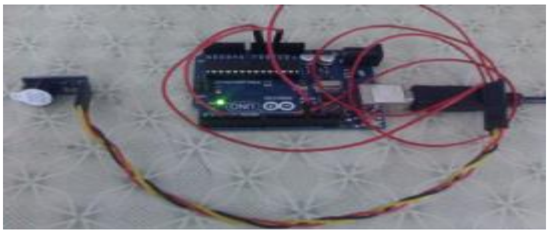


Fig. 2: Shows the test result

The 5V requirement can be met by the Arduino board itself. However, for the 12V-5A power supply, we need an additional circuit. A 15-0-15V center tap transformer is used in this power supply. After that, we use a bridge rectifier circuit that converts AC power to DC power.

The DC current we get after the conversion is not ripple free, so two 3300 µF capacitors C1 and C2 = 0.33 µF are used to remove ripple. The voltage regulator LM338K is used to regulate the voltage of the power supply unit, which supplies a regulated voltage of 12 V and a constant current of 5 A.

The 100 µ F capacitor C3 is used to remove output voltage ripples and diode D3 is used to protect the circuit when capacitor C3 begins to discharge. Figure 9 shows the circuit diagram of the 12V, 5A power supply.

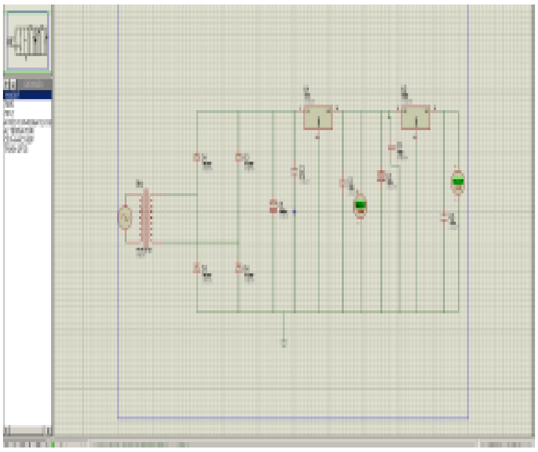


Fig. 3: Circuit diagram

7. CONCLUSION

The ANN is one of the most reliable techniques for future calculations. The model shows that it can be very useful in classifying speech signals. It works more like a human brain than conventional computer logic. ANN has better speech recognition rates than MFC, but the algorithm is complex to train and dynamically sensitive, which can cause problems. The future of this technology is very big and the only thing that can be improved is hardware development as ANN needs faster hardware. The automation system based on speech recognition was built and implemented. The system was specially developed for patients with paralysis and also for the elderly. An adjustable wooden bed with a motor is very economical and affordable. The adjustable bed offers two lifting positions, the sleeping position and the sitting position. Depending on the comfort of the patient, he can simply select the desired position by saying it, which acts as voice commands for the system. The use of voice commands eliminates the need for remote controls and other electronic devices and makes it easier to interact with the system to perform the function and control the devices. With the buzzer, the patient can alert the guardian if the patient needs help. The LED can be used for various purposes; can be used to indicate the needs of multiple patients.

REFERENCES

1. Arthi.J.E and M.Jagadeeswari, "Control of Electrical Appliances through Voice Commands," IOSR Journal of Electrical and Electronics Engineering, vol. 9, pp. 13-18, February 2014.
2. Norhafizah bt Aripin and M. B. Othman, "Voice Control of Home Appliances using Android," in International Conference on Electric Power, Electronic, Communication, Control, And Informatic Systems, Malang ,pp. 142-146, August 2014.
3. Rajesh Khanna Megalingam, Ramesh Nammily Nair, and Sai Manoj Prakhya, "Automated Voice based Home Navigation System for the Elderly and the Physically Challenged," in International Conference on Advanced Communication Technology, Seoul, pp. 603-608, February 2011.
4. Parameshachari B D, Sawan Kumar Gopy, Gooneshwaree Hurry and Tulsirai T. Gopaul., "A Study on Smart Home Control System through Speech," International Journal of Computer Applications, vol. 69,pp. 30-39, May 2013.
5. T.Kirankumar and B. Bhavani, "A Sustainable Automated System for Elderly People Using Voice Recognition and Touch Screen Technology," International Journal of Science and Research (IJSR), vol. 2, pp. 265-267, August 2013.

DUAL-BAND MICROSTRIP PATCH ANTENNA WITH EBG STRUCTURE AT THE GROUND PLANE TO IMPROVE THE BANDWIDTH AND RETURN LOSS

Dr I. Selvamani[1]., B.Lohitha [2]., B.Madhuri [3]., B.Lahari [4]., B.Bavitha [5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ : i.selvamani@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0410 , 15RG1A0411, 15RG1A0412, 15RG1A0413), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— The future development of personal communication devices aims to provide images, voice and data anywhere in the world, anytime. This shows that future antennas of communication terminals must meet the broadband requirements in order to effectively cover all possible operating bands. The aim of this article is to improve the bandwidth and return loss of a rectangular microstrip patch antenna using an EBG structure at the ground plane. EBG structures are periodic arrangements of dielectric materials and metallic conductors in the ground plane of antennas. Mounted microstrip antennas can only radiate a small part of their energy into free space, as more energy is filtered through the dielectric substrate. In order to improve the efficiency of the antenna, the propagation through the substrate must be restricted so that the antenna can emit more power in the direction of the main beam and thus improve its efficiency. To design this we used the CST software tool. The technical antenna offers a significantly improved bandwidth of 51.2 MHz and a return loss of -15.15 dB at 2.446 GHz and a bandwidth of 77.4 MHz as well as a return loss of -39.02 dB at 3.8875 GHz compared to the conventional rectangular microstrip patch antenna with a bandwidth of 26 MHz and a return loss of -19.16 dB at 1.806 GHz and a bandwidth of 28 MHz and a return loss of -14.24 dB at 2.2677 GHz..

***Keywords*— CST computer simulation technology, EBG electromagnetic band gap structure, medical and scientific ISMB industrial tape, microstrip patch antenna, bandwidth, return loss, wireless communication.**

1. INTRODUCTION

Antennas are one of the basic components for wireless communication. The Webster dictionary defines an antenna as "a generally metallic device for transmitting or receiving radio waves" [1]. Wireless communication has increased rapidly and continuously in recent years. A large number of users are increasing every day, but the available bandwidth is limited. As a result, engineers strive to optimize their devices for greater capacity and improved quality coverage. Microstrip antennas have a major narrow bandwidth disadvantage, but wireless communication applications require high bandwidth and relatively high gain [2].

Microstrip antennas are flat resonant cavities that filter and radiate through their edges. Circuit board techniques are used to store antennas on flexible substrates to produce inexpensive and reproducible low profile antennas [3]. For good antenna performance, a thick dielectric substrate with a low dielectric constant is desirable because it offers better efficiency. Many techniques have been used to improve bandwidth by interpolating the terrain modification in the antenna configuration [4].

2. ANTENNA DESIGN

We consider a conventional single-layer microstrip rectangular patch antenna. The dimensions of this classic patch antenna were assumed to be length L = 30 mm and width W = 30 mm. The FR4 is used as the substrate for the antenna design. The dielectric constant of FR4 is 4.3, the loss tangent is 0.025, and the thickness is 1.6 mm. The coaxial probe delivery technique was used to stimulate the patch. The design and simulation process was carried out with CST MWS Version 2012. The geometry of the conventional rectangular microstrip patch antenna is shown in Figure 1.

Table -1: Dimensions of the conventional antenna

NAME	VALUE	DESCRIPTION
f_o	2.4GHz	Operating Frequency
h	1.6 mm	Height of Substrate
ϵ_r	4.3	Dielectric Constant
Lg	50 mm	Length of ground
Wg	70 mm	Width of ground
L	29.778626 mm	Length of patch
W	38.393444 mm	Width of patch
t	0.038 mm	Thickness of patch
F	(5mm,6mm)	Feed Points

Fig 1 shows the structure of a conventional microstrip patch antenna, while FIG. 2 shows the design of the proposed microstrip patch antenna with an EBG structure embedded in the ground.

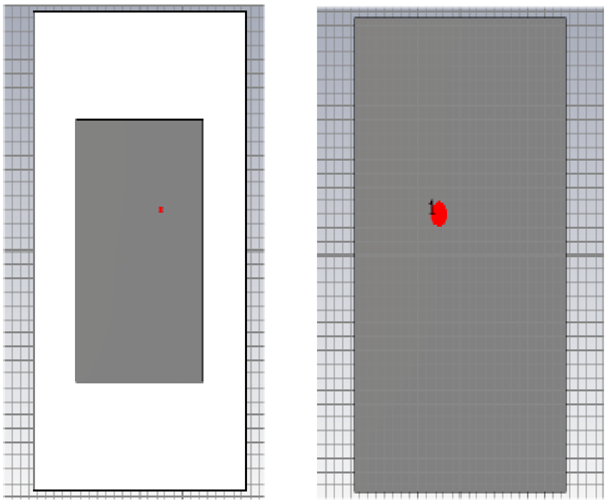


Fig. -1: Conventional microstrip patch antenna with front and rear views

In the proposed antenna we introduced 4 holes each 5mm x 5mm in size in the ground plane and a 2mm x 10mm slot in the patch as shown in Figure 2.

Table -2: Dimensions of the proposed antenna

S.No	Parameters	Dimensions
1.	Substrate	L_S=57.50 mm W_S=46.50 mm H_S=1.6 mm
2.	Holes in patch	4 square holes of each 5mm x 5mm at corner
3.	Holes in ground plane	4 square holes of each 5mm x 5mm at corner
4.	Feed points	(6 mm, 6 mm) from origin
5.	Slot in Patch	2mm x 10mm

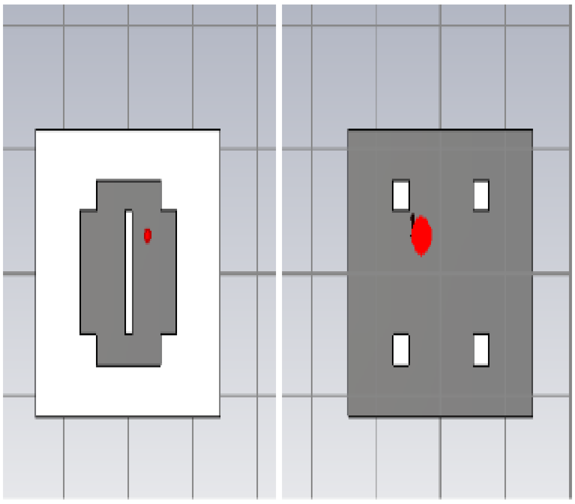


Fig. -2: Structure of the proposed microstrip patch antenna with EBG structure, showing a front and rear view

3. RESULTS AND DISCUSSIONS

The conventional microstrip patch antenna is first simulated using the CST software. This simulated antenna has a bandwidth of 26 MHz and a return loss of -19.16 dB at 1.806 GHz and a bandwidth of 28 MHz and a return loss of -14.24 dB at 2.2677 GHz. As shown in Figure 3, the total bandwidth value for this antenna is 54 MHz, so the traditional antenna has a narrow bandwidth. Therefore, further modifications are required to improve bandwidth and return loss.

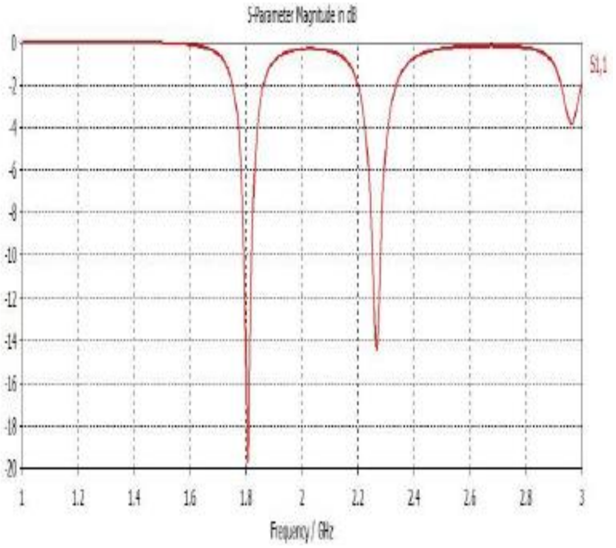
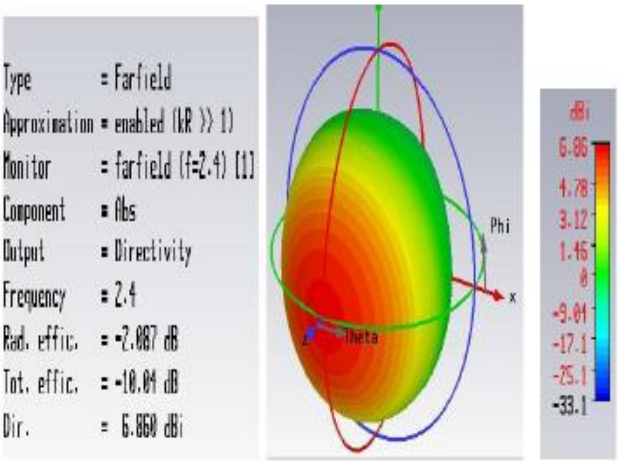


Fig. -3: Variation of the return loss (dB) depending on the frequency (GHz) of the conventional antenna



Type = Farfield
Approximation = enabled (kR >> 1)
Monitor = farfield (f=2.4) [1]
Component = Abs
Output = Directivity
Frequency = 2.4
Rad. effic. = -2.087 dB
Tot. effic. = -10.04 dB
Dir. = 6.860 dBi

Fig. 4: Conventional antenna radiation pattern

Fig. 5 shows the variation in return loss (dB) as a function of frequency (GHz) for the proposed antenna. It shows that it has a bandwidth of 51.2 MHz and a return loss of -15.15 dB at 2.446 GHz and a bandwidth of

77.4 MHz and a return loss of -39.02 dB at 3 and 8875 GHz, respectively. The total bandwidth value for the proposed antenna is 128.6 MHz, which is much better than the traditional micro-band patch antenna. This shows that the introduction of EBG into the ground plane improves the antenna's performance.

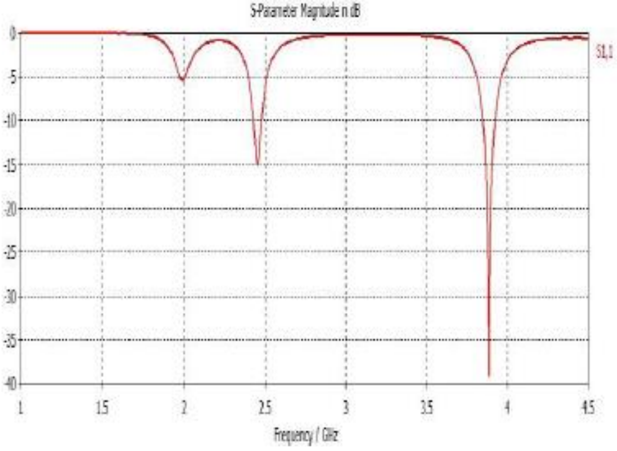


Fig. -5: Variation of the return loss (dB) depending on the frequency (GHz) of the proposed antenna

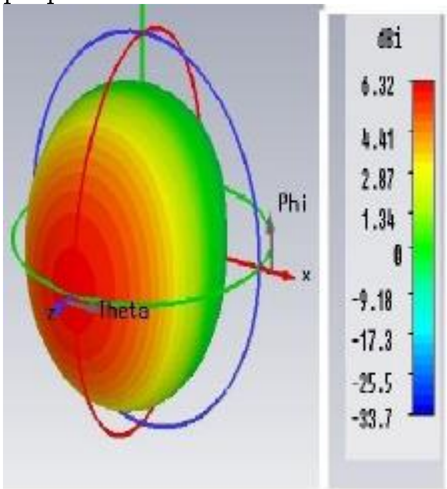


Fig. -6: Radiation diagram of the proposed antenna

Table -3: Comparison between the two antennas

TYPE	RETURN LOSS	BW	VSWR
Conv. Rect. Micro. Patch Antenna	(a) -19.66 dB at 1.806 GHz (b) -14.24 dB at 2.2677 GHz	(a)26 MHz (b)28 MHz	(a)1.230 (b)1.483
Proposed Micro. Patch Antenna	(a)-15.15 dB at 2.446 GHz (b) -39.02 dB at 3.8875 GHz	(a)51.2 MHz (b)77.4 MHz	(a)1.333 (b)1.022

4. CONCLUSION

From the above results and the discussion, it can be concluded that the microstrip patch antenna with EBG structure provides better performance in terms of bandwidth and return loss compared to the conventional microstrip patch antenna. The desired level of optimization has been achieved. The antenna offered can be used for a variety of ISM band applications such as Wi-Fi devices and other wireless applications, bluetooth devices, many defense and medical applications. It can also be developed for different application modes with different frequencies in the future by reducing the dimensions of the patches and significantly improving the bandwidth and return loss.

REFERENCES

1. "IEEE Standard Test Procedures for Antennas", IEEE Std. 149-1979, Institute of Electrical and Electronics Engineers, New York, 1979.
2. Alka Verma, "EBG structures and its recent advances in Microwave Antenna" publication in "International Journal of Scientific Research Engineering & Technology (IJSRET)", Vol-1 Issue-5, pp. 084-090, Aug 2012.
3. C.A. Balanis, "Antenna Theory: Analysis and Design", 3rd Edition, Willey 2005.
4. CST Tutorial, "Microwave Studio Computer Simulation Technology", 2006.
5. R. Garg, P. Bhartia, I. Bahl, A. Ittipiboon, "Microstrip Antenna Design Handbook", Arteck House, 2001.
6. William H. Hayt, Jr. John A. Buck, "Engineering Electromagnetic", 6th Edition, McGraw-Hill, 2001.
7. Sandeep Kumar, Subodh Kumar Tripathi, Nitin Kumar, Rachit Aggarwal, "Design of Microstrip square-patch antenna for improved Bandwidth And Directive gain" in "International Journal of Engineering Research and Applications (IJERA)", Vol-2, Issue-5, pp. 441-444, Mar- April 2012.

R.J. James and P.S. Hall, "Handbook of Microstrip Antennas", IEEE Electromagnetic waves series 28, 1989.

IMPLEMENTATION OF DOUBLE PRECISION FLOATING POINT MULTIPLIER USING XILINX VIRTEX-5 FPGA

Rajkumar chunchu[1]., E.Pavani [2]., G.Anusha [3]., G.Harika [4]., K.Sushmitha [5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- chunchurajkumar@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0433, 15RG1A0435, 15RG1A0441, 15RG1A0468),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— ***Every computer has an accurate floating point processor or accelerator that meets the precision requirements with full floating point arithmetic. Decimal numbers are also known as floating point numbers because a single number can be represented by at least one significant digit, depending on the position of the decimal point. In this article, we describe an implementation of the IEEE 754 double precision floating point multiplier that targets the Xilinx Virtex-5 FPGA. The platform used here is Verilog. The multiplication process used here is pipelining, which gives the latency of eleven clock cycles***

Keywords— Double Precision, Multiplier, Verilog, Floating Point, VLSI

1. INTRODUCTION

The floating point representation contains an encoding that contains three basic parts: the mantissa, the exponent, and the sign. This involves using binary numbering and powers of 2, resulting in a floating point number representation configured as single-precision (32-bit) and double-precision (64-bit) floating-point numbers. Both numbers are identified by the IEEE 754 standard. As stated in the IEEE 754 standard, a single precision number has one sign bit, 8 exponent bits, and 23 mantissa bits, while a double precision number has one sign bit, 11 exponent bits, and implies 52 mantissa bits. In most applications we use a 64-bit floating point to avoid losing precision in a long sequence of operations that are used for the calculation. The mantissa has a hidden main bit wrapped around it and the rest are division bits. The most common arrangements represented by this standard are the single and double precision floating point number parameters. In each cell, the head number indicates the number of bits used to represent each part, and the numbers in square brackets indicate the bit positions stored for each segment in single and double precision numbers.

2. PROPOSED SYSTEM

The floating point multiplier is implemented here without the use of DSP segments. The A and B inputs are divided into sign (64th bit), exponent (63 - 52nd bit) and mantissa (51 - 0 bit). "Xor" the character from a & b gives the last character. Both inputs are checked whether one or both are equal to "0", infinite. This is done with two if - else statements. These checks are required to handle exceptions. The implicit "1" is concatenated with the mantissa of a & b and the 53 partial products are calculated. Each partial product is calculated as the "y" mantissa of a, with each mantissa bit of b being replicated 53 times. To add in this way, the number of partial products must be a power of 2. Since 53 is not a power of 2, the partial products are divided into 32 + 16 + 4 + 1. Each group is added in the above method. And the resulting 4 sub-products are added with the required compensation. Among the 4 groups, the fourth group is the same as the 53rd sub-product, since this group only contains the final sub-product.

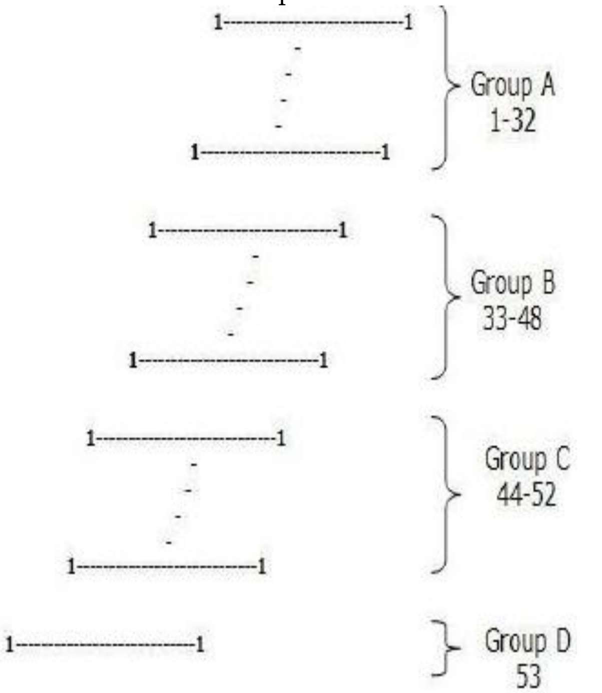


Figure 1: Division of 53 sub-products into 4 groups.

By adding 2 adjacent partial products, for example: p3 and p4 in FIG. 2, the LSB of p3 remains the same. Therefore, adding p3 and p4 concatenates the LSB of p3 (p3 [0]) to the right of the sum of p3 (52: 1) and p4.

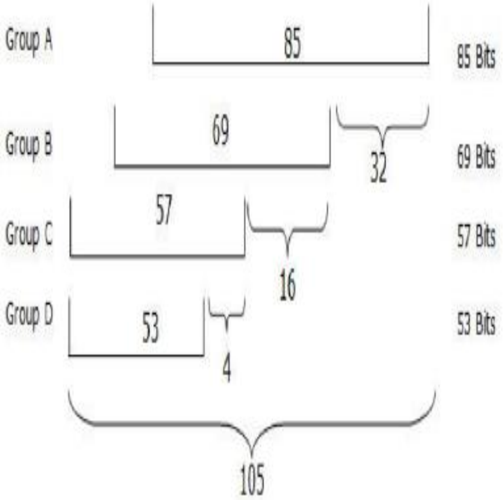


Figure 2: The last four intermediate products with their offsets

The remaining four intermediate sub-products with their offsets are shown in Figure 4. Grouping and adding as in the previous cases creates critical paths. Therefore, the data is split horizontally as shown in Figure 3.

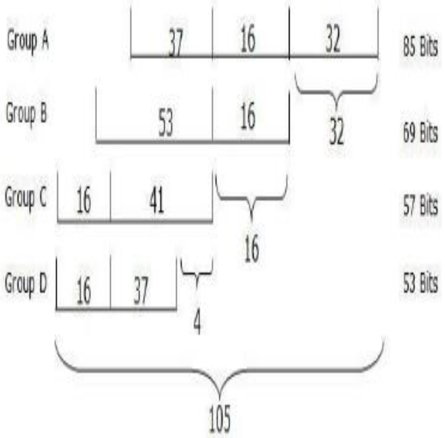


Figure 3: The last four intermediate products with horizontal division

The 32 least significant bits (0 - 31) of group A do not need to be added. Group A bits (32-47) and Group B bits (0-15) are added. The remaining 37 bits (48-84) of group A and bits (16-68) of group B are added with the transfer from the previous horizontal partition. The three horizontal partitions are each as w, x and y assigned.

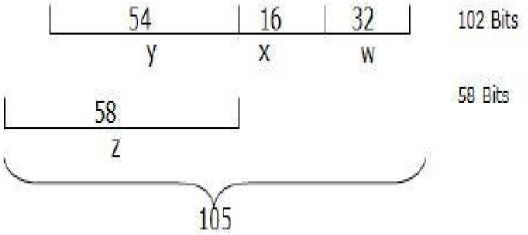


Figure 4: Group AB and Group CD with remuneration

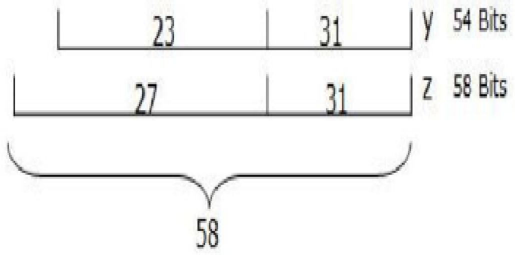


Figure 5: Horizontal division of Y and Z.

If w and x are left unchanged, then y and z are again divided into two parts, as shown in Figure 6, and added. The results are recorded again in the eighth stage of the pipeline. Then the result of the multiplication is obtained by concatenating the intermediate results of w, x and (y + z). The MSB is then checked. If it's zero, it should be shifted one left. Only one shift is required as only standard entries are taken into account. Bit 105 is always one when bit 106 is zero. The results are recorded again in the ninth stage of the pipeline.

3. SIMULATION AND SYNTHESIS

The ability to simulate HDL programs is critical to HDL design. The simulation enables an HDL description of a design (called a model) to successfully pass the design review. This is an important reference that passes the intended function of the design (specification) to the implementation of the code in the HDL description. In addition, it allows you to explore the architecture. The detailed RTL logic (Register Transistor) of the double precision floating point multiplier is shown in Figure 8.

In this RTL, the number of cut registers used is only 10% of the total Virtex 5 FPGA kit, ie; Out of 28,800 only 3129 slice registers are used. Here the number of input and output latches used is 69. The number of slices used here is only 19 %, ie; 1388. The number of logics used is 10%, that is; 3150

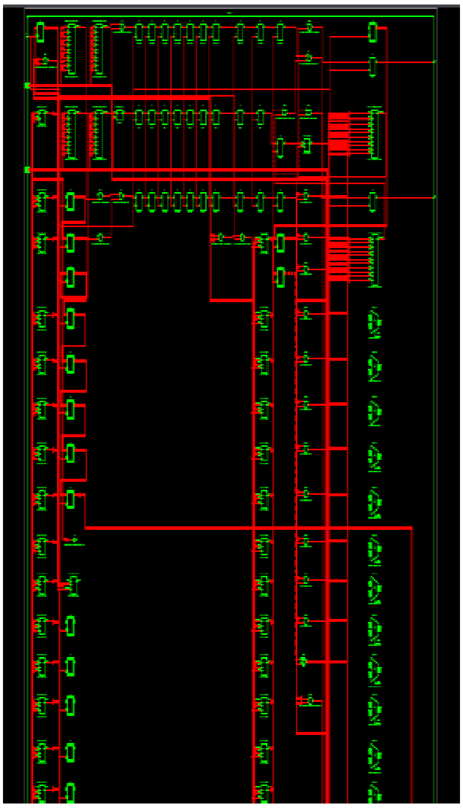


Figure 6: RTL diagram

4. REALIZED RESULT

Table 2 Result of the Virtex5 implementation (without using DSP segments)

Logic utilization	Used	Available	Utilization
Number of Slices	3129	28,800	10%
Number of Slice LUTs	4779	28,800	16%
Number of used as Logic	3150	28,800	10%
Number of Occupied Slices	1388	7,200	19%
Number of fully used LUT-FF pairs	3101	4,807	64%
Number of Bounded IOBs	198	480	41%
IOB Flip Flops	69		
Number of BUFG	1	32	3%

4.2 Time overview

In this time summary analysis the multiplier used is used with no DSP slots. The maximum synthesis frequency that we get here is 141.33 MHz. The maximum clock frequency used by this project is 115.65 MHz. The design frequency here is 108.69 MHz. The minimum delay time is 3488 nanoseconds. The minimum arrival time of the entrances in front of the clock: 3549 nanoseconds. The minimum required exit time after the clock: 2775 nanoseconds.

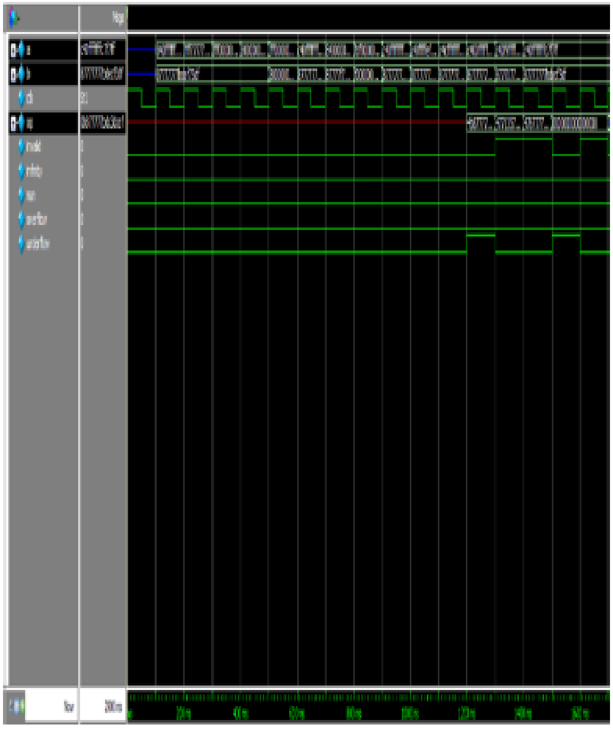


Figure 7: wave simulation form (I) QuestaSim 10.0B

5. CONCLUSIONS

In this project, the double precision floating point multiplier works successfully on FPGAs in light of the IEEE-754 format. The modules are made of Verilog HDL for better use in FPGA. In this implementation, the maximum frequency of the multiplier performed by the channelization algorithm won the maximum frequency. Since the main idea behind this implementation is to increase the speed of the multiplier by reducing the delay in each stage using the optimal tube design, it has the advantage of less delay compared to another method. The results obtained with the proposed calculation and use is better in terms of speed and material used. The maximum synthesis frequency that we get here is 141.33 MHz. The maximum clock frequency used by this project is 115.65 MHz. The design frequency here is 108.69 MHz. The minimum delay time is 3488 nanoseconds. The latency is 11 clock cycles.

REFERENCES

1. A.P. Ramesh, A. V. N. Tilak, A. M. Prasad ”An FPGA Based High Speed IEEE-754 Double Precision Floating Point Multiplier Using Verilog ”

published in IEEE 978-1-4673-5301-4/13/© 2013IEEE.

2. A.Jaenicke and W. Luk,"Parameterized Floating-Point Arithmetic on FPGAs", Proc. Of IEEE ICASSP,2001, vol. 2, pp. 897-900.
3. M. Al- Ashrafy, A. Salem and W. Anis,"An Efficient Implementation of Floating Point Multiplier " Electronics Communications and Photonics Conference(SIECPC) 2011 Saudi International, pp.15,2011.
4. IEEE 754 Standard for floating-point arithmetic, ANSI/IEEE Std 7541985 Vol ,Issue , 12 Aug 1985.
5. N. Shirazi , A. Walters, and P. Athanas, " Quantitative Analysis of Floating Point Arithemetic on FPGA Based Custom Computing Machines," Proceedings of the IEEE Symposium on FPGAs for custom computing machines(FCCM"96),pp.107-116,1996.
6. J. G. Prokais and D. G. Manolakis (1996),"Digital Signal Processing: Principles, Algorithms and Applications", Third Edition.
7. D. H. Tabassum, K. S. Rao, "Design of double precision floating point multiplier using vedic multiplication", International Journal of Electrical and Electronics Research, vol. 3, Issue 3,pp(162-169), july-september 2015.
8. F.de Dinechin and B. Pasca. "Large multipliers with fewer DSP blocks in Field Programmable Logic and Applications". IEEE, Aug. 2009.
9. B. Lee, N. Burgess. "Parameterisable floating point operations" Cardiff School of Engineering, Cardiff University, Cardiff CF243TF U.K. 07803-7576-9/02 © 2002 IEEE.
10. B. Fagin and C. Renard, "Field Programmable Gate Arrays and Floating Point Arithmetic," IEEE Transactions on VLSI, vol.2, no. 3, 365-367, 1994.

DESIGN OF DATA COMMUNICATION SYSTEM FOR USB & PARALLEL USB IN XILINX VHDL

N Umamaheshwari[1]., M.Pavani [2]., N.Sushma [3]., P.Ravalika [4]., P.Spandhana[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- umaece05@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0482, 15RG1A0496, 15RG1A04A4, 15RG1A04A7), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— The USB system is used to communicate between computer peripherals and the host computer. The programming of Xilinx devices takes our concept from concept to software simulation. The ISE 13.2 Project Navigator processes our multilevel design inputs to perform an ISE design simulation. In our Xilinx 13.2 project we are using the ISE13.2 simulator which contains the signals in the waveforms of the test bench. In the current work, normal USB and parallel USB are used for communication. Parallel USB reduces processing delay and improves communication speed. In our proposed work, we implement a parallel processing unit in the USB host that allows the host to reduce the processing delay and increase the overall communication speed. The existing USB stack is implemented unchanged, but the processing unit of the stack is changed and switched in parallel. The internal DMA engine and triangular architectures are the components that we are working on in parallel to improve the results..

***Keywords*— USB, Xilinx ISE (embedded software environment) 13.2 .**

1. INTRODUCTION

USB stands for Universal Serial Bus. This is the network connection and connected to the host computer. There are two types of attachments. They are called functions and hubs. The function includes peripheral devices such as mice, printers, etc. Hubs contain peripheral devices such as the dual power point adapter, which converts components from a plug to USB. Each device contains the number of the endpoint. These are the sources and destinations for communication between the host and the device. Each function needs to know the data element and the host computer needs to know where the signals are coming from. Therefore, numbers are assigned to each component on the USB. Each device contains the number of the endpoint. These are the sources and destinations for communication between the host and the device. Hubs and functions are commonly referred to as devices. The combinations of endpoint numbers and addresses are designed for a conventional PC configuration. You need to know where the signals are coming from.

Types of data transfer

When communicating over USB, we need to understand the different types of data that are transferred over USB.

I . Transmission control:

The function of the control transfer file type is to configure, control, and check the status of a USB device. The host sends the request to the device and the corresponding data transfers are tracked on the appropriate lines.

ii. Isochronous transfers:

The USB has enough time to handle the maximum flow of data. USB offers a special type of data transfer. It guarantees a constant transmission speed with the required bandwidth. This isochronous transmission method uses unidirectional lines with no error handling procedures.

2. LITERATURE SURVEY

Several research articles from various journals and conferences have been reviewed, and a review of the existing literature in the proposed field is reported below:

2.1 Panday et al. (2013) designed USB 2.0 with a great focus. It contains both low-level programming functions (JTAG) and application-level functions, that is, high-level programming functions (Linux). The limitation of the JTAG approach is that the based approach is suitable for low-level programming. It is issued due to the amount of code that is written for each function. Therefore, the states of the system that can be checked in the middle stage are very slow. Limitation of the Linux-based approach Linux code is very large. He's running really big. Activate different modules in the background. The number of attempts is extensive. Various problems go unnoticed or get squeezed. The status of the system cannot be checked in the intermediate stage. It should be required for debugging.

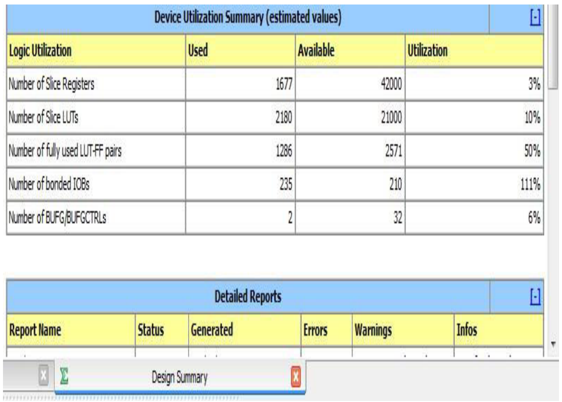
2.2 Act Przemys et al. (2012) designed the concept of USB. This concept is designed by implementing a hardware description language. Offers a simulation model. The code can be synthesized at the same time. It can be physically of your own finite state machine. The conceivable solution is division. The architecture depends on the direction of data transmission.

2,3 Jolfaei et al. (2009) developed USB 2.0 for high speed and are an easy-to-use peripheral interface. The Spartan 3 FPGA hardware implementation is used. Has the ability to manage data easily

3. EXECUTION OF THE PROPOSED WORK

Various development tools are used for the implementation of our project. The implementation of our project includes test bench signal waveform generation, simulation, cycle and design summary, etc. The ISE (Integrated Software Environment) 13.2 software is used to design the circuits and code verification. The development of the test bench and the diagrams of the modules are also designed by our software. The Xilinx device is programmed with this software via a design input. There are several steps involved in the ISE design flow in the processes of this ISE Project Navigator.

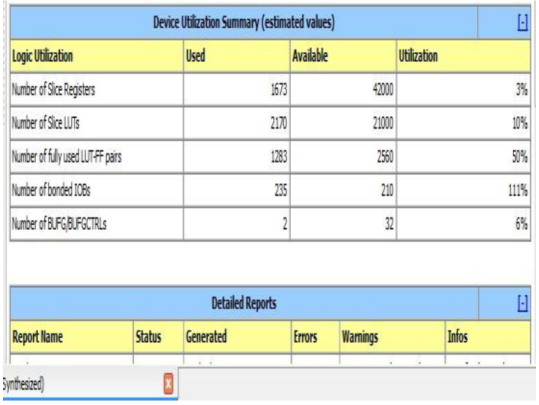
Table No. 1. Test stand for normal USB



Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	1677	42000	3%
Number of Slice LUTs	2180	21000	10%
Number of fully used LUT-FF pairs	1286	2571	50%
Number of bonded IOBs	235	210	111%
Number of BUFG/BUFGCTRLs	2	32	6%

Detailed Reports					
Report Name	Status	Generated	Errors	Warnings	Infos

Table no. 2. Test bench for parallel USB



Device Utilization Summary (estimated values)			
Logic Utilization	Used	Available	Utilization
Number of Slice Registers	1673	42000	3%
Number of Slice LUTs	2170	21000	10%
Number of fully used LUT-FF pairs	1283	2560	50%
Number of bonded IOBs	235	210	111%
Number of BUFG/BUFGCTRLs	2	32	6%

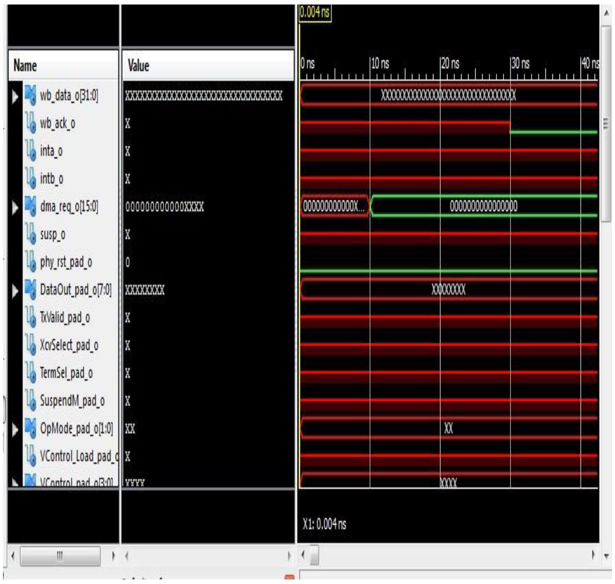
Detailed Reports					
Report Name	Status	Generated	Errors	Warnings	Infos

The Xilinx ISE 13.2 simulator provides a result in the form of a test bench that contains the waveform signal. It can be used to simulate modules. USB designers work on serial processes in all communication. Since USB works in the serial protocol, we cannot change the communication process, but we can change the internal processing of USB. Due to the change in the internal processing of the USB, the processing time is shortened. Therefore, because of the shortening of the processing time, there is an improvement in the communication speed. We implement the parallel processing unit in the USB host. As a result, the processing time is reduced and the overall communication speed is increased. The existing USB stack is implemented unchanged. However, the batch processing unit is modified and executed in parallel. Wish bone architecture and internal DMA engine are the components that help with parallel processing to improve the end result.

Plan of work

1. Creation of CRC modules
2. Development of the Wishbone architecture
3. Development of an internal DMA
4. Development of standard USB
5. USB upgrade through parallel processing

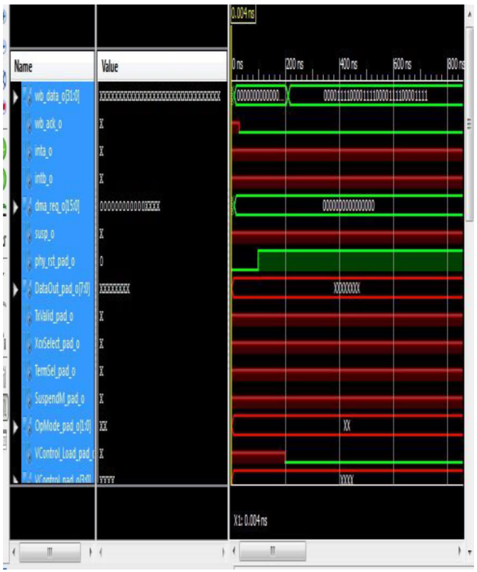
4. ANALYSIS AND COMPARISON OF THE RESULTS



Name	Value
wb_data_o[31:0]	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
wb_ack_o	X
inta_o	X
intb_o	X
dma_req_o[15:0]	000000000000XXXX
susp_o	X
phy_rst_pad_o	0
DataOut_pad_o[7:0]	XXXXXXXX
TxValid_pad_o	X
XcvSelect_pad_o	X
TermSel_pad_o	X
SuspendM_pad_o	X
OpMode_pad_o[1:0]	XX
VControl_Load_pad_o	X
VControl_pad_o[3:0]	XXXX

Fig 1 signal that is generated on normal USB

In order to build the Hi-Speed USB kernel, we had to implement the USB 2.0 specification, which only specifies the language spoken by Hi-Speed USB but does not provide implementation details. Therefore, our first goal was , the VHDL code to complete that implements the Hi-Speed USB specification protocol. As part of the specification, we want our kernel to support all three speeds of USB devices.



Name	Value
wb_data_o[31:0]	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
wb_ack_o	X
inta_o	X
intb_o	X
dma_req_o[15:0]	000000000000XXXX
susp_o	X
phy_rst_pad_o	0
DataOut_pad_o[7:0]	XXXXXXXX
TxValid_pad_o	X
XcvSelect_pad_o	X
TermSel_pad_o	X
SuspendM_pad_o	X
OpMode_pad_o[1:0]	XX
VControl_Load_pad_(	X
VControl_pad_o[3:0]	XXXX

Fig 2 signal is generated in parallel via USB

5. CONCLUSIONS

The Universal Serial Bus (USB) was developed to connect the number of peripheral devices to the PC. USB 2.0 has uses across the industry. It is a host-oriented protocol. You are using a physical serial bus. It is controlled by the host. Basic data transfer is the core specification of USB 2.0. The USB specification defines three data rates. In other words, at low speed. Top speed and high speed. We have implemented the simulation of normal USB and parallel USB in the Xilinx ISE 13.2 software. The result is verified with the generation and signaling of the test bench . We implement a parallel processing unit in the USB host, which allows the host to shorten the processing time and increase the overall communication speed.

REFERENCES

1. Jolfaei, F. A., Mohammad izadeh, N., Sadri, M. S., & FaniSani, F. (2009, December). High speed USB 2.0 interface for FPGA based embedded systems. In Embedded and Multimedia Computing, 2009. EM-Com 2009.
2. Pandey, M. K., Shekhar, S., Singh, J., Agarwal, G. K., & Saxena, N. (2013, July). A novel approach for USB2. 0 validation on System on Chip. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-4). IEEE .
3. USB 2.0 Transceiver Macrocell Interface (UTMI): International Co Retrieved from http://www.intel.com/technology/usb/download/2_0_xcvr_macrocell_1_05.pdf
4. Babulu, K., & Rajan, K. S. (2008, July). FPGA Implementation of USB Transceiver Macrocell Interface with USB2. 0 Specifications. In Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on (pp. 966-970). IEEE.
5. Jan Axelson, USB Complete - Everything you need to develop custom USB peripherals, Lakeview research, 3rd Edition, Aug 2005.
6. "Spartan-3 FPGA Family: Complete Data Sheet", Xilinx Corp., Aug 2005.

SMART SHOPPING SYSTEM USING RFID AND QR CODES FOR BILLING AND ELECTRONIC PAYMENTS

Dr.Archek Praveen Kumar[1]., N.Ramyasree [2]., N.Deepika [3]., N.Swapna [4]., N.Roshini [5]
1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- archekpraveen@gmail.com)
2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0491, 15RG1A0492, 15RG1A0493, 15RG1A0494),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— Most of us spent what seemed like forever in a retail store waiting for the person in front of us to check in lots of items when we just needed a loaf of bread or a single shirt. Long lines at the checkout can result in people waiting long before paying for their goods and leaving, no matter how many items are purchased. We believe that this can be changed, and our idea is automating the payment process, enabling automatic payment and aiming for a new digital shopping experience. We offer this with a smartphone app that allows the user to scan the products they want to buy, generate the invoice for any products scanned, make payment and just leave the store. This process ensures easy management of customers, inventory, and finances, which makes management and customers happy. This app helps you to avoid long queues and to pay easily. Not only do they reduce waiting time, but they also reduce or eliminate the need for a cashier. In addition, according to the current trend of electronic transactions, the whole process will be cashless.

***Keywords*— QR Code, Smart Shopping, RFID, RFID Reader, Bluetooth**

1. INTRODUCTION

The idea of the project is to optimize this purchasing process in a retail store so that the customer can manage the payment process. So far, the approach to automated purchasing and invoicing has been more hardware-driven. Several attempts have been made to design intelligent shopping carts with various functions. Awati and Awati [1] have developed a design that aims to eliminate the need to move heavy carts and automate the billing process, regardless of any fraud. Yew et al. [2] describes a system for intelligent shopping that replaces the conventional barcode with RFID tags and scanners. In 2013, another approach was proposed to use wireless sensor networks to design a cart where all processing is done locally on the cart and a camera that acts as a barcode reader [3]. Most of the other related jobs also use RFID-based shopping carts that interact with various sensors. Our approach is to provide customers with a better shopping experience by saving time, minimizing labor in the mall, and at the same time dramatically increasing operating costs by eliminating complex hardware and allowing the user to make their purchases. Just use your smartphone and allow the retail store to keep track of customer purchases.

2. DISADVANTAGES OF THE EXISTING MODEL

We believe that the current purchasing system for retail stores has not changed significantly and that the model we offer can help improve the customer's shopping experience. Customers have to wait an extremely long time during the ordering process , no matter how many items they pick up in the store. This is especially true when the people in front of you are counting your money or vouchers incredibly slowly and during the sale. The invoicing process in a store is the most tedious part of shopping and we believe it can be eliminated. When it's your first time in a department store , finding a specific product can be a tedious task.

In addition, retail stores traditionally use barcodes to identify each product as well as their membership cards. In terms of data storage barcodes can contain less data, mostly digital, and more space claim, as they one-dimensional are . If a barcode is damaged or dirty, it cannot read data and cannot be scanned properly.

We believe that the entire system can be modified through digital solutions to provide a better shopping experience for both the customer and the management.

3. PROPOSED SYSTEM

We offer a system with a mobile app that can be downloaded on any smartphone, combined with an RFID authentication system to fully digitize the buying process. We recommend using QR codes to identify products in- store instead of barcodes. Because QR codes have three positions and recognition patterns, they can be read faster and at a greater distance, which enables faster payment. Since they data both horizontally as to store and vertically, they can store the same amount of data in less space than a barcode. In addition, QR codes can contain different types of data, such as: B. Numbers, symbols, text and verification codes.

So in a large store, this would mean a significant reduction in the storage space required. In addition, if the QR is damaged, it can still be scanned and recover over 30% of the data, making it superior in terms of data recovery. The suggested system components are listed below:

The architectural diagrams of the two components of the proposed model are given below.

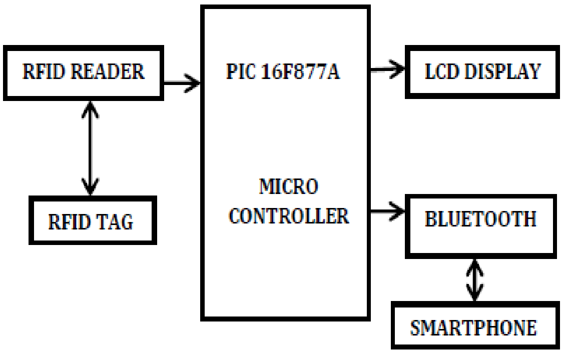


Fig 1 Hardware architecture

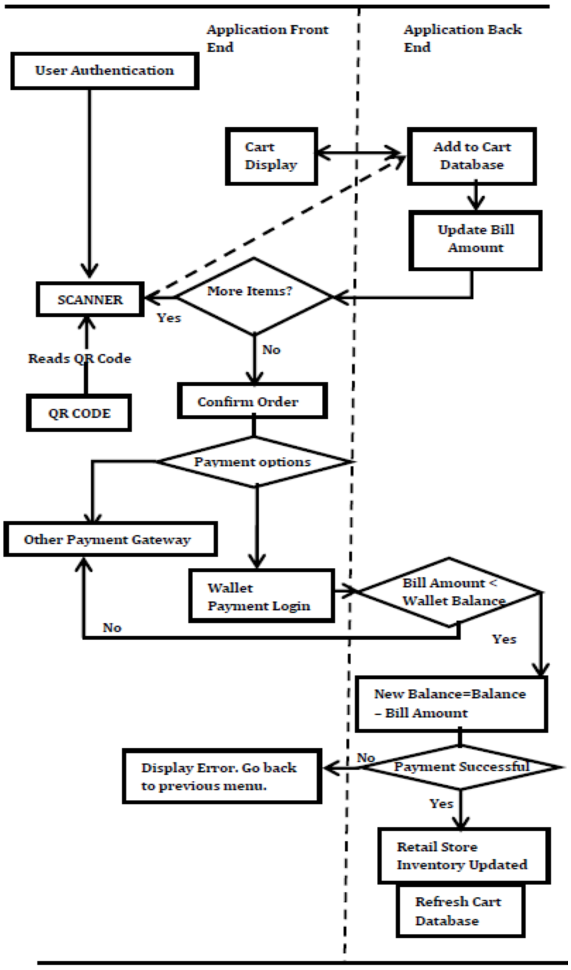
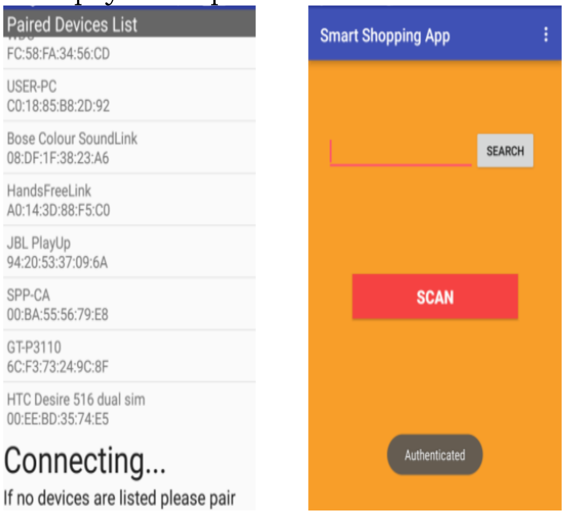


Fig. 2: Software flow diagram

4. RESULT ANALYSIS

The smartphone application provides a user interface (UI) for interacting with the products and for adding, displaying or deleting a personalized shopping cart. The customer can access the smartphone application to make purchases once they have been authenticated via Bluetooth. The application uses a QR code scanning function that accesses the camera of their smartphone and allows the user to retrieve a product, scan its QR code and thus add it to the shopping cart. The UI screen will be updated with the current product details and the automatic total bill increase. The user interface also offers the option of selecting an item and removing it from the shopping cart. The app can also tell users which area of the store a particular product is in. This way, the user can quickly find what they are looking for and avoid long queues to review their articles. outside . There is also the option of paying registered members by wallet. As soon as you have signed up and you have sufficient credit, the invoice amount will be deducted from your wallet. Otherwise, they will be redirected to other payment options.


Paired Devices List

FC:58:FA:34:56:CD

USER-PC
C0:18:85:B8:2D:92

Bose Colour SoundLink
08:DF:1F:38:23:A6

HandsFreeLink
A0:14:3D:88:F5:C0

JBL PlayUp
94:20:53:37:09:6A

SPP-CA
00:BA:55:56:79:E8

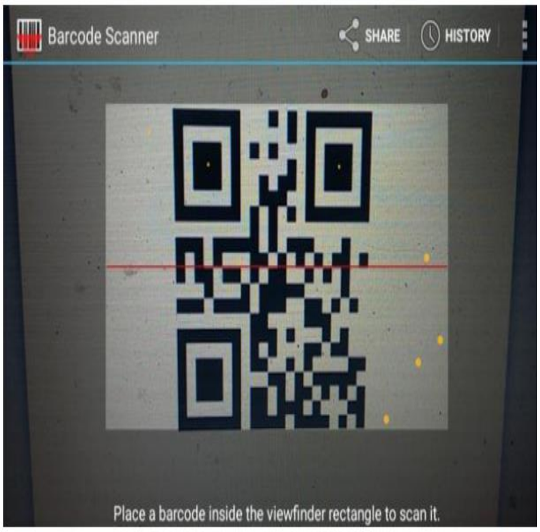
GT-P3110
6C:F3:73:24:9C:8F

HTC Desire 516 dual sim
00:EE:BD:35:74:E5

Connecting...

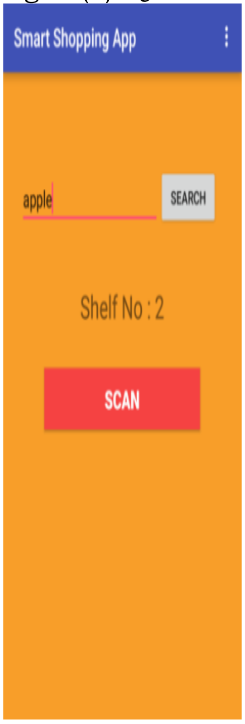
If no devices are listed please pair

Fig. 3 (a): Application authentication via Bluetooth



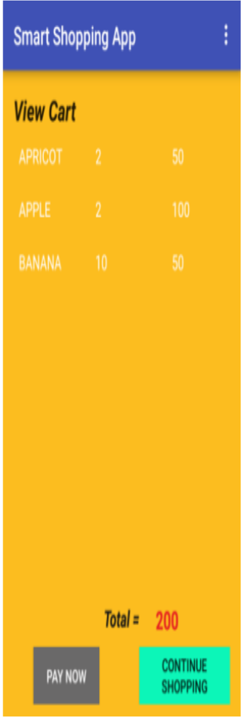
Place a barcode inside the viewfinder rectangle to scan it.

Fig. 3 (b): QR scan of the product



Shelf No : 2

Fig. 3 (c): Search option

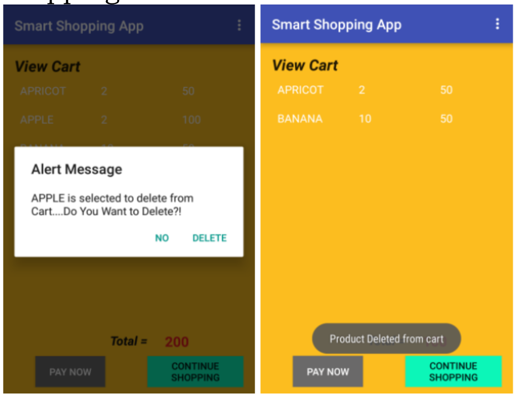


View Cart

APRICOT	2	50
APPLE	2	100
BANANA	10	50

Total = 200

Fig. 3 (d): Show shopping cart



View Cart

APRICOT	2	50
APPLE	2	100

Alert Message

APPLE is selected to delete from Cart....Do You Want to Delete?!

Total = 200

View Cart

APRICOT	2	50
BANANA	10	50

Product Deleted from cart

Fig. 3 (e): Take out of the basket

The RFID system is implemented to speed up the ordering process to improve and both the user as to offer the management a better shopping experience. It consists of a microcontroller as the central unit, which is connected to an RFID reader and a Bluetooth module. An integrated card with an RFID tag is used for user authentication. The card is scanned at the entrance and allows the mobile application to authenticate the application using Bluetooth technology to make purchases. Retail stores currently use personalized barcode cards to identify registered members. The advantage of using RFID over barcodes is that no line of sight for communication required for RFID. This means that a customer only has to be very close to the reader and be authenticated.

5. CONCLUSION

We believe that this purchasing process can revolutionize the existing procurement system, as there is no very expensive investment for the store management is. Almost everyone has a smartphone with a camera, that 's all that is needed to automate the software we offer. In return, the speed of purchase and the convenience for the customer are immense. This results in a win-win situation where the customer is happy to come back for the convenience of this system and management is happy with the customer loyalty. The scope of the idea is also immense when used in conjunction with predictive algorithms. By tracking the data generated by the app, stores can use data mining to personalize the entire shopping experience for each person and display personalized messages to customers based on their buying habits. You can also use the prediction to tell the user what they might have forgotten to buy while visiting the store.

REFERENCES

1. S. Sainath, K. Surender, V. Vikram Arvind," Automated Shopping Trolley for Super Market Billing System", International Journal of Computer Applications 0975 – 8887, ICCCMIT-2014.
2. Sonali S. Dhokte, Bhagyashree S. Patere, Megha T. Magar, Vaidehi S. Kulkarni , Prashant S. Patil , Prof. Rajesh A. Patil, "Smart Shopping Trolley Using Rechargeable Smart Card", ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 5, May 2015.
3. L. Yew, L. Fang, C. Guancheng, C. Jianing, and L. Hangzhi, "RFID: Smart

Shopping for the future," Singapore Management University, Tech. Rep.

4. J.Awati and S.Awati, "Smart Trolley in Mega Mall," vol.2, Mar 2012.
5. "Zebra Crossing (Zxing) Bar Code Scanner Project for Android "https://github.com/zxing/zxing.

Shivani Titarmare , Monali Thakre , Rasika Shingote, Sakshi Shukla, Vikram Deshmukh, "RFID Based Smart Shopping Trolley with IR Sensor", 2017 IJSRST , Volume 3 ,Issue 2, Print ISSN: 2395-6011

SMART IOT BASED REAL-TIME ENERGY MANAGEMENT IN WSN USING ZIGBEE PROTOCOL AND ETHERNET SHIELD

Manasa konda[1]., T.Deepika [2]., T.Bhavya latha [3]., T.Gayatri [4]., U.Anusha [5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- kondamanasa26@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A04C9, 15RG1A04D0, 15RG1A04D1, 15RG1A04D2), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— : In this document we report on an efficient implementation of the Internet of Things to monitor home appliances. Introduction of a real-time energy management system based on wireless sensor networks for controlling and monitoring the energy consumption of household appliances in private households. The current sensor and the voltage sensor are electrically charged in order to detect current and voltage and to calculate the current consumption of electrical devices. This data is transmitted wirelessly to the Ethernet shield using the ZigBee protocol. The transmitted data is remotely monitored and controlled by IOT. This allows the user a flexible remote control mechanism over a secure web connection to the Internet. This system helps the user to control electrical devices automatically, manually and remotely via a smartphone or a PC. This system is very efficient, economical and flexible in its operation and can therefore reduce electricity costs for consumers.

Keywords— IOT, Energy management, home automation, wireless sensor network, ZigBee, Ethernet Shield.

1. INTRODUCTION

Electrical energy is the main source of development and advancement in this technological world. The technology develops the energy demand and the energy demand increases day by day. This energy demand occurs both in the domestic and in the industrial sector. According to the latest annual energy report, electricity demand in residential areas is expected to increase by 24% in the coming decades, while the global electricity consumption trend will also continue to increase. The demand for electrical energy is increasing and fossil fuels are decreasing due to increased energy consumption. In addition, the discrepancy between supply and demand and the lack of automation and monitoring tools have already resulted in significant power outages around the world. As we have seen, with the installation of more household appliances and consumer electronics, energy consumption in residential areas is increasing dramatically.

2. LITERATURE SURVEY

Guangming Song and Aiguo Song present the design and implementation of a home surveillance system based on hybrid sensor networks. The system follows a three-tier architecture that combines hybrid node networks with web access. An improved sensor node was designed and manufactured to provide controlled mobility to wireless sensor networks. The mobile node can perform simple aircraft movements and is easy to control via various user interfaces. A test bench with the static nodes and the mobile node was also created to validate the basic functions of the proposed hybrid sensor network system. The network repair and event tracking functions of the mobile sensor node were tested. The stability of the system, which is offered for long-term house monitoring tasks, was also checked.

Meng-Shiuan Pan and Lun-Wu Yeh proposed an intelligent lighting control system based on WSN for interiors. Wireless sensors are responsible for measuring the current illuminance. Two types of lighting fixtures are used, full lighting and local lighting fixtures, to provide backlights and headlights, respectively. Users can have different lighting needs depending on their activities and profiles. A lighting requirement is the combination of background and focused lighting requirements and the location of the users. We consider two requirement models, namely binary satisfaction and continuous satisfaction models, and propose two decision algorithms to determine the appropriate lighting of devices and to achieve the desired optimization goals. A closed loop device control algorithm is then applied to adjust the illuminance levels of the lighting fixtures. The results of the prototyping confirm that our ideas are practical and achievable.

Khusvinder Gill and Shuang-Hua proposed a home automation system based on ZigBee. This technology offers exciting new opportunities to improve the connectivity of devices in the home for home automation purposes. In addition, with the rapid expansion of the Internet, there is additional potential for remote control and monitoring of these network-connected devices. However, the introduction of home automation systems has been slow. This document details the reasons for this slow takeover

3. PROPOSED SYSTEM

The current sensor and the voltage sensor are connected to the household appliances to measure the electrical parameters of the household appliances. The energy consumption of each device is calculated using the measured current and voltage. Refer to the following sections for details on how to design and develop the proposed system. Figures 3.1 and 3.2 describe the functional description of the developed system. The ZigBee module is used for the wireless transmission of electrical parameter data that is recorded by the sensor modules. The ZigBee transmitter is connected to various reliable data receiving and recording devices on one side of the ZigBee module receiver. The ZigBee receiver was connected to one another via the serial interface of the Ethernet Shield. The data collected by the Ethernet shield was sent to the LAN by the wireless router. Household appliances can be monitored and controlled remotely. The control operation is carried out in three ways. These are manual control, automatic control and remote control.

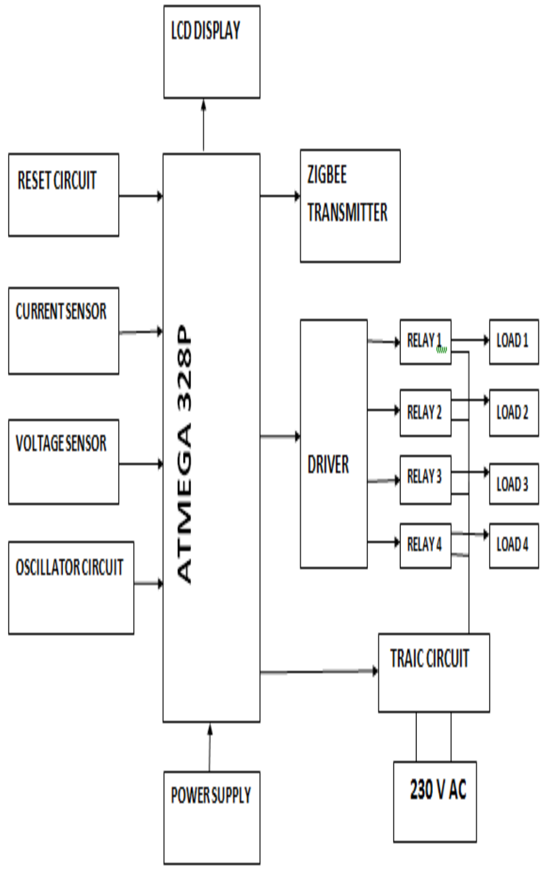


Fig. 3.1: Section "Intelligent Power Management System Transmitter"

1) Automatic control: With automatic control, the devices can be controlled with intelligent software based on the conditions of the electricity tariff. In this mode, the user can save power by automatically switching the devices according to the preset power consumption.

2) Manual control: An on / off switch is located directly on the devices. In this mode, the user can operate the devices manually without following the automatic command. The manual control is very flexible.

3) Remote control: Remote control allows the user to remotely interact with the devices through a smartphone or PC through a secure connection to the Internet. The user can operate the devices when they are not at home. This feature also reduces manual effort and time by controlling all devices from one place.

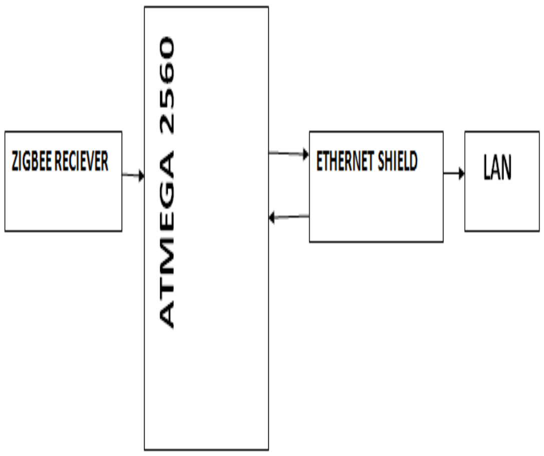


Fig. 3.2: Receiver section of the intelligent energy management system

The Ethernet Shield is an Arduino-compatible expansion card ("shield") with which your Arduino can communicate as a client or server over an Ethernet network.

4. RESULT ANALYSIS

A transmission protocol is used to wirelessly transmit the collected data. In order to transfer the data, it must have low power consumption, consist of several devices in the network and offer high-performance communication. Zigbee is a standard WPAN 802.15.4 protocol that transmits data over a distance of 100 m. It consumes less power and can be operated in three different frequency bands (2.4 GHz, 915 MHz, 868 MHz). A ZigBee network consists of a coordinator and terminals. It supports a maximum of 65,000 devices in a ZigBee network. The data speed is 256 kbps. It is generally suitable for detection and control applications. In the ZigBee network, the end devices are the sensor nodes that communicate wirelessly with the coordinator in the form of a mesh topology.

The router is connected to the RJ45 jack controller. It is a network device that transfers data packets between computer networks. Routers perform the functions of "directing traffic" on the Internet. Typically, a data packet is transmitted from one router to another via the ATmega 328 is a single-chip microcontroller developed by Atmel in the Mega AVR family. It is widely used in standalone projects and systems where a simple microcontroller with low power consumption and low cost is required. Perhaps the most common implementation of this chip is the popular Aurduino development platform. The current sensor is a device that detects the electrical current in a cable and generates a signal proportional to it. Here we are using a 1000: 1 current transformer which has a high saturation point, high temperature stability and high resistance to the voltage range.

5. CONCLUSION

An intelligent power management system based on the IOT was developed. This system monitors and controls the energy consumption of household appliances automatically, manually and remotely via a wireless network. The system is easy to design, uses less power, and is portable in size at a low cost. Thus, real-time monitoring of electrical devices can be accessed via a website. In the future, the system can be expanded to monitor the entire institute, schools, colleges, companies, etc.

REFERENCES

1. Erol-Kantarci and H. T. Mouftah, “Wireless sensor networks for cost efficient residential energy management in the smart grid,” IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 314–325, Jun. 2011.
2. K. Gill, S. H. Yang, F. Yao, and X. Lu, “A zigbee-based home automation system,” IEEE Trans. Consumer Electron., vol. 55, no. 2, pp. 422–430,May 2009.
3. Nagender Kumar Suryadevara, Subhas Chandra Mukhopadhyay, Sean Dieter Tebje Kelly, and Satinder Pal Singh Gill „WSN-Based Smart Sensors and Actuator for Power Management in Intelligent Buildings” 1083-4435, 2014 IEEE.
4. F. Benzi, N. Anglani, E. Bassi, and L. Frosini, “Electricity smart meters interfacing the households,” IEEE Trans. Ind. Electron., vol. 58, no. 10,pp. 4487–4494, Oct. 2011.
5. P. Cheong, K.-F. Chang, Y.-H. Lai, S.-K. Ho, I.-K. Sou, and K.-W. Tam,“A zigbee-based wireless sensor network node for ultraviolet detection of flame,” IEEE Trans. Ind. Electron., vol. 58, no. 11, pp. 5271–5277, Nov.2011.
6. G. Song, Z. Wei, W. Zhang, and A. Song, “A hybrid sensor network system for home monitoring applications,” IEEE Trans. Consumer Electron.,vol. 53, no. 4, pp. 1434–1439, Nov. 2007.
7. M. S. Pan, L. W. Yeh, Y. A. Chen, Y. H. Lin, and Y. C. Tseng, “A WSN based Intelligent light control system considering user activities and profiles,” IEEE Sensors J., vol. 8, no. 10, pp. 1710–1721, Oct. 2008.
8. D. Man Han and J. Hyun Lim, “Smart home energy management system Using IEEE 802.15.4 and zigbee,” IEEE Trans. Consumer Electron., vol. 56, no. 3, pp. 1403–1410, Aug. 2010.

GESTURE HUMAN MACHINE INTERFACE USING MEMS ACCELEROMETER AND A FLEX SENSOR FOR EASY USER INTERFACE

N Uma Maheshwari[1]., B.Aswini [2]., B.Shruthika [3]., S.Nandhini [4]., S.Sireesha [5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- sanjeevsagar163@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0409, 15RG1A0414, 15RG1A04B5, 15RG1A04B6),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The hand gesture-based control of electronic devices is growing in importance today. Most electronic devices focus on the hand gesture recognition algorithm and user interface. The Human Machine Gesture Interface (GHMI) uses an accelerometer and a flexible sensor. GHMI is mainly based on the hand gesture recognition algorithm used to control electronic / electrical devices. The hardware module consists of an accelerometer, a flexible sensor, a bluetooth model, a Raspberry Pi and an Arduino kit. Hand gestures are determined by the accelerometer and the flexible sensor. These signals are transmitted wirelessly to the Raspberry pi with the Bluetooth model HC-05. The Raspberry Pi receives and processes the data sent by the Bluetooth model. It also consists of relay and bypass plates to support the equipment. In home automation, when the end user presses the door switch, they receive a text message informing them that someone is at the door.

Keywords— Accelerometer, Flex sensor, Bluetooth model, Raspberry pi and Arduino

1. INTRODUCTION

Gesture is defined as a movement of a limb or other part of the body performed to emphasize speech. It can also be defined as an action or comment made as a sign of attitude. A gesture is scientifically divided into two different categories: dynamic and static. A waving hand means that leave an example of a dynamic gesture is and a stop sign is an example of a static gesture. It is necessary to explain all static and dynamic gestures over a period of time in order to understand the whole message. Gesture recognition is the interpretation of human movements using a computing device. The hand movement can be detected by a controller, the accelerometer and flexion contains, in order to detect the inclination and acceleration of the movement.

The basic purpose of the gestural human-machine interface (GHMI) is to provide a means of controlling electronic devices through hand gestures. The GHMI acts as a remote control for operating all entertainment electronics devices in a household. However, this is accomplished through hand gestures rather than pressing buttons. Gestures can be made through the use of sensors, i. H. Accelerometer, Flex , etc., can be detected. The gesture recognition based on an accelerometer carries out a time domain comparison or a modeling. Recognized and recognized hand gestures are used as control signals for controlling devices.

GHMI is a device that replaces all other portable remote controls used in private homes and performs all of its functions. In homes, remote controls are typically used for household appliances such as televisions, CD players, air conditioners, DVD players, and music systems. GHMI can as a remote control for controlling on / off lights, door openers, etc. used to be. All of these devices can be controlled from GHMI. The wireless technology used at GHMI will revolutionize the way people view digital devices in our homes and offices. This wireless technology is useful in home environments where there is an infrastructure to connect electrical devices. This technology is suitably used for low cost home automation.

2. LITERATURE SERVEY

Android software is used to control home applications. With Android software we can control apps like lights, fans, televisions and other apps. [1] GHMI uses hand gestures instead of Android software. The VPL DataGlove was built by Thomas Zimmerman, who also patented the flexible optical sensor used by the gloves. The DataGlove was a cloth glove with two fiberglass loops on each finger. If a user has a particularly large or small hand, the loop will not match the actual position very well and the user will not be able to make an accurate gesture. There is an LED at one end of each loop and a photo sensor at the other end. Valdimir Vujoic explains the implementation of the sensor as Internet of Things (IOT) using Raspberry Pi. The IOT technology offers various advantages such as security, cost savings, etc. In this project the IOT is used for door security. When the doorbell is pressed, a message is sent to mobile device owners indicating that someone is at the door. [3]

3. OBJECTIVES

The main objectives of this project are :

1. Detection of a simple hand movement by various sensor modules.
2. Design and implementation of intelligent gloves to detect hand movements.
3. Face recognition for the door unlocking system.
4. Update the end user by sending a message over a Wi-Fi broadcast.

4. PROPOSED SYSTEM DESIGN

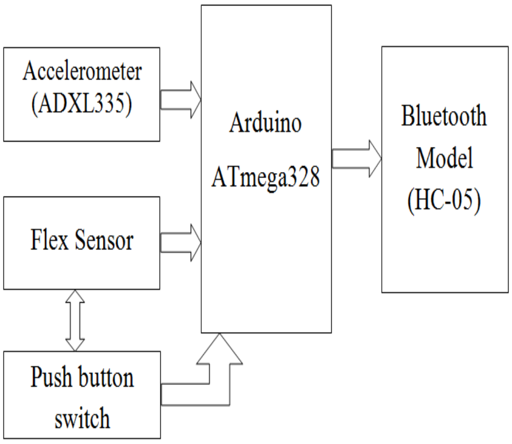


Fig. 1: Section of the GHMI transmitter

In the transmitter section, the Arduino Uno is used as the main controller , i.e. H. The heart of the transmitter. There are different sensors like the flex sensor, the accelerometer to generate the gesture. Gestures are recognized with the help of these sensors. The occurrence of this event is updated from the sending side to the receiving side.

The accelerometer is used to select the device to be turned on, and the flexible sensor is used to turn the device on and off.

In the transmitter area, the HC-05 bluetooth module is used for serial communication, which is used to send the hand movement detected by Flex and to send the accelerometer to the receiver area.

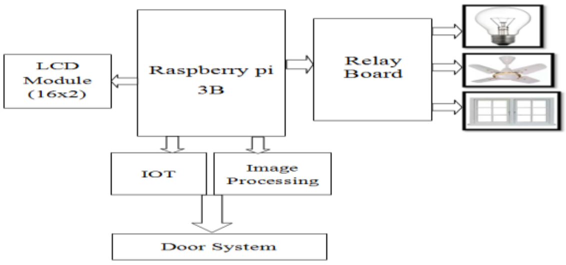


Fig. 2: Section of the GHMI receiver

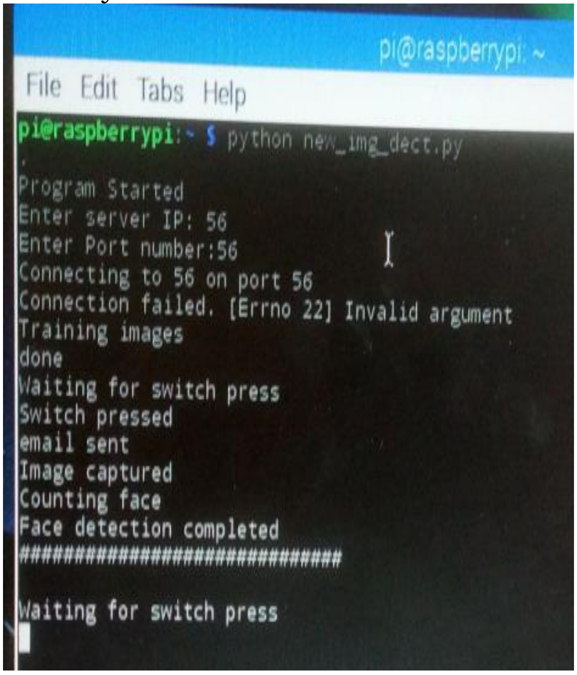
In the Receiver section, Bluetooth is used to receive message packets related to the occurrence of an event on the sender side.

In the receiver module is the physically connected device to be controlled. There are various devices such as lights, fans and windows that can be controlled wirelessly without buttons. Various relay cards are used in this section. This relay card is used to control devices.

Door security for home automation is guaranteed through the use of IOT concepts and powerful image processing algorithms for authentication and authorization.

6. RESULTS ANALYSIS

With the camera installed in the door, the image captured by the camera is compared with the image stored in the database of authorized people in the house. After processing and comparing the image, the authorized person has access and an updated message is sent to the owner regarding the presence of a person at the door. The email with the photo, the fixed SMS format and a personal phone call is generated by the system to inform you that the switch has been pressed. For security reasons, a photo of an unauthorized person is taken and emailed to the owner. GHMI (Gesture Home Machine Interface) is mainly used to help people with physical disabilities control their home application through hand gestures using a flex and accelerometer sensor. The proposed system offers great comfort and convenience to people with disabilities through the use of the GHMI system.

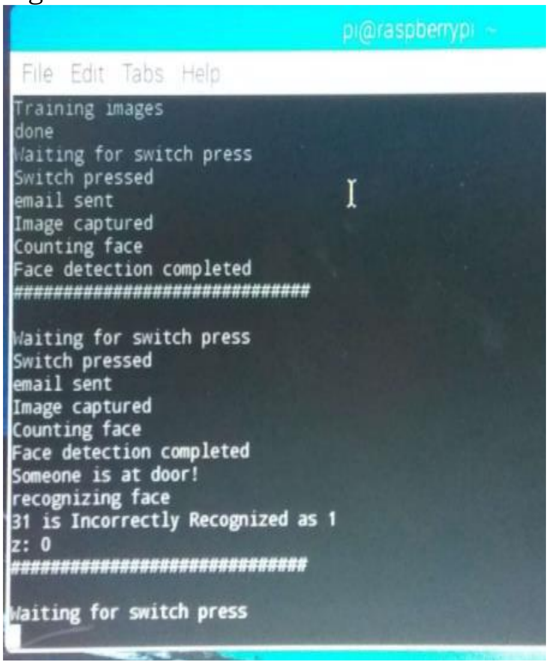


```
pi@raspberrypi:~ $ python new_img_dect.py

Program Started
Enter server IP: 56
Enter Port number:56
Connecting to 56 on port 56
Connection failed. [Errno 22] Invalid argument
Training images
done
Waiting for switch press
Switch pressed
email sent
Image captured
Counting face
Face detection completed
################################

Waiting for switch press
```

Fig. 5: Person in front of the door



```
Training images
done
Waiting for switch press
Switch pressed
email sent
Image captured
Counting face
Face detection completed
##############################

Waiting for switch press
Switch pressed
email sent
Image captured
Counting face
Face detection completed
Someone is at door!
recognizing face
31 is Incorrectly Recognized as 1
z: 0
##############################

Waiting for switch press
```

Fig. 6: Person in front of the door

7. CONCLUSION

GHMI (Gesture Home Machine Interface) is mainly used to help people with physical disabilities control their home application through hand gestures using a flex and accelerometer sensor. The proposed system offers great comfort and convenience to people with disabilities through the use of the GHMI system. GHMI is implemented using the concept of IOT and image processing. GHMI can also provide home security by authenticating the person's identity. The proposed systems make it easier for the gesture-based wireless system to control household appliances that can also be used for industrial applications.

REFERENCES

1. Valdimir Vujoic, MirjanaMakshimovic, “Raspberry Pi a sensor Web node for home automation” Elsevier on Computer and Engineering 42(2015).
2. Gantt, Charles. “Raspberry Pi Camera Module Review Tutorial Guide” TweakTown News. Tweak Town, 2 2013. Web. Oct. 2013.
3. Shiguo Lian,Wei Hu, Kai Wang, “Automatic User State Recognition for Hand Gesture Based Low-Cost Control System”,IEEE,2014.
4. Deepali Javale,Mohd Mohsin,Shreerang Nandanvar, Mayur Shingate,”Home automation & security using Android ADK”,International Journal of Communication and Computer Technology (IJECCT) Volume 3 Issue 2 ,March 2013.

PARALLEL CASCADED CLASS A&B CMOS LINEAR POWER AMPLIFIER FOR WIMAX APPLICATIONS

Narmada kari [1]., M.Anjali [2]., M.Shivani [3]., M.Sravya reddy [4]., M.Lahari [5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- narmadakari@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0477, 15RG1A0479, 15RG1A0480, 15RG1A0481), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— CMOS power amplifiers are an area of interest to designers today due to the high demand for mobility requirements with higher data transfer speeds. Countries are the most energy consuming part and the main culprit in the transceiver chain. Since we have a limited power source for lithium batteries for mobile communication, more effort for more innovative ideas and better performance of designs to improve performance will be recognized. CMOS is an area of interest for its cost and integration benefits. This article introduces the CMOS linear power amplifier for WiMAX applications for a frequency of 2.5 GHz. To increase linearity and efficiency, a class A & B power amplifier is used in parallel cascade. The power amplifier power stage with 1 volt supply offers a maximum output power of 0.45 mW and an additional energy efficiency of 29% with a gain of 33.4 dB at an operating frequency of 2.5 GHz.

Keywords— CMOS power amplifier, parallel class A&B power amplifier, transformer, power combiner, WiMAX.

1. INTRODUCTION

The rapid growth of wireless systems has resulted in an increasing demand for smaller, lower cost systems with superior and complex functionality. This demand has prompted the search for single-chip transceivers made in CMOS technology. In WiMAX front-end circuits, the power amplifier is an important component that determines the transmission coverage and the overall efficiency of the system. The most critical points in power amplifier design are linearity and efficiency. Because of the complex modulation technique, which uses phase and amplitude modulation to transmit data as far as possible for the given bandwidth, high linearity is required, while high efficiency improves thermal management, reliability, cost and battery life . This article introduces a fully integrated, high output power amplifier using Class AB in parallel for WiMAX applications in standard 90 nm technology.

III. PROPOSAL FOR A HIGH-PERFORMANCE AMPLIFIER

The complete block diagram of the proposed power amplifier is shown in FIG. The proposed power amplifier consists of an input balun, a control stage, an impedance matching network between the stages, a power stage and a combined power transformer (pct). Input balun in Fig. It is an electronic device that converts an unbalanced signal into a differential. The application of the balun is to connect an unbalanced signal to a balanced transmission line for long-distance communication.

A double step is used to provide sufficient gain. The controller and the power stages are designed in a cascade topology. In addition, the pilot stage is biased in class A to increase the overall linearity of PA. The impedance matching network is placed between the controller and the power stage in order to maximize the power transferred from the controller to the power stage. In the power stage, two combinations of class AB power amplifiers are used in a cascade topology where the top PA combination is similar to the bottom combination.

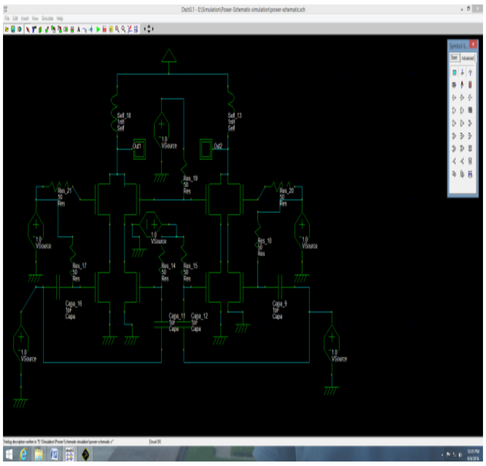


Fig. 1Power stage of the power amplifier

$$g_{mA\&B} = g_{mA} + g_{mB}$$

Power combiner as a method of increasing the output power, matching the impedance and converting the differential into a terminated signal in a power amplifier circuit. In our circuit, the transformer is used as a power combiner that combines the output of various amplifiers.

III. SIMULATION RESULT

The simulation of the power level of the proposed circuit, provided according to the layout diagrams of the combinations of transistors and their analog representation, is simultaneously given below.

With a 1 V supply in the power stage, the simulation result showed a drain current of 380 µA and an output power of 0.45 mW and a transistor voltage of 1.2 V.

$$PAE = 100 \times \frac{P_{out}^{RF} - P_{in}^{RF}}{P_{DC}^{Total}}$$

PAE - Aggregate Energy Efficiency (PAE) is a metric for evaluating the efficiency of a power amplifier that takes into account the effect of the amplifier gain. It is calculated (in percent) as follows:

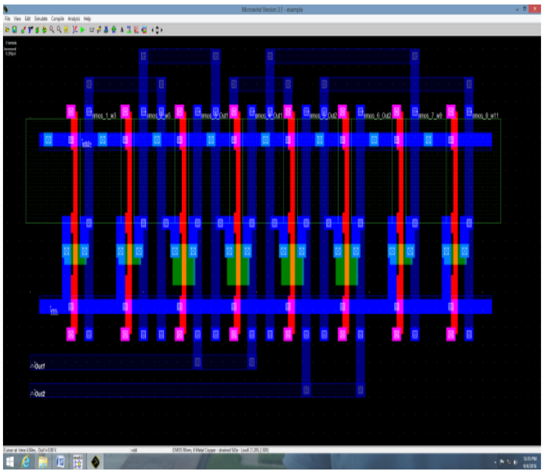


Fig. 2 Structure of the configuration of the power level simulation

It is generally defined as the average ratio between the amplitude or power of the signal at the output port and the amplitude or power at the input port. It is often expressed in units of logarithmic decibels (dB) ("dB gain"). A gain greater than one (greater than zero dB), i.e. H. A gain, is the defining property of an active component or circuit, while a passive circuit has a gain less than one.

$$gain(db) = 10\log\left(\frac{P_{out}}{P_{in}}\right) dB$$

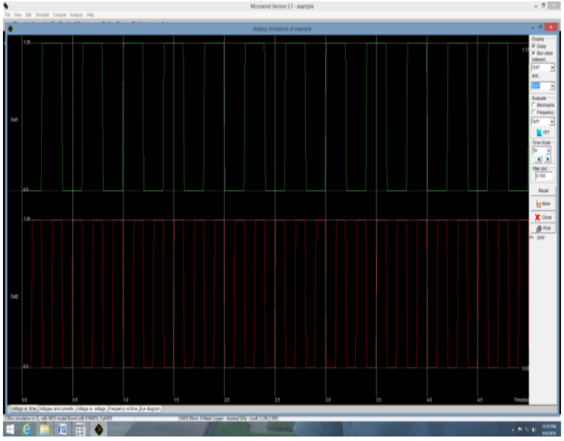


Fig. 3 Analog simulation of the proposed power level

As we know, the output power is an important factor for the WiMAX application because the coverage area depends on the output power. As we know, it is the power in watts produced by the circuit at its loads, given by the mathematical expression:

Power = voltage × current

An average output power of 0.45 mW is thus obtained with a drain voltage of 1.2 V and a drain current of 380 uA at the output of the power stage.

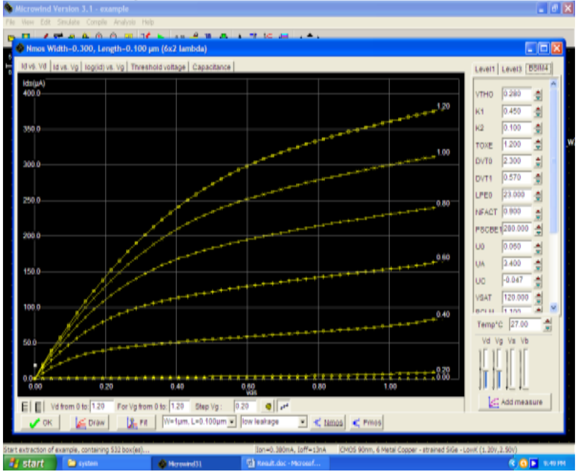
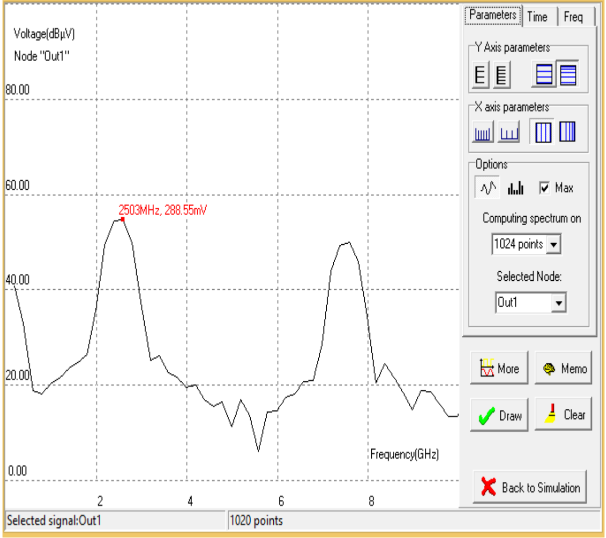


Fig. 4 Current graphic of the simulation result

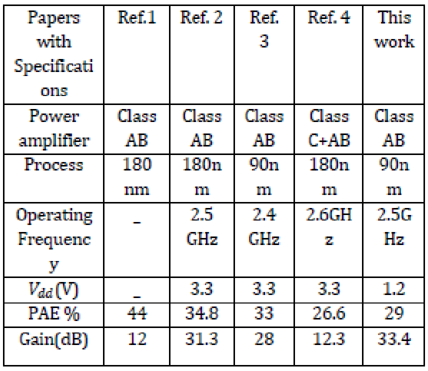


Selected signal:Out1 1020 points

Fig. 5 Output spectrum of the power amplifier

With the power supply, the proposed power amplifier generates a maximum output power of 0.45 mW and a PAE of 29% is achieved at maximum output power. The power amplifier provides a gain of 33.4 dB. The power amplifier is offered for the WiMAX signal (802.16e), which offers the good linearity required for WiMAX.

Table 1- comparison between articles



Papers with Specifications	Ref.1	Ref. 2	Ref. 3	Ref. 4	This work
Power amplifier	Class AB	Class AB	Class AB	Class C+AB	Class AB
Process	180 nm	180nm	90nm	180nm	90nm
Operating Frequency	-	2.5 GHz	2.4 GHz	2.6GHz	2.5GHz
V_{dd} (V)	_	3.3	3.3	3.3	1.2
PAE %	44	34.8	33	26.6	29
Gain(dB)	12	31.3	28	12.3	33.4

IV. CONCLUSION

This article introduces a linear CMOS power amplifier in standard 90 nm technology. A modified parallel power amplifier is proposed to increase efficiency and linearity. The output of these power amplifiers is interconnected by an off-chip power transformer. The power stage of the proposed power amplifier offers an output power of 0.45 mW and a PAE of 29% with a gain of 33.4 dB for a frequency range of 2.5 GHz with a power supply of 1 V for the WiMAX application.

REFERENCES

1. Manoj Sharadrao Awakhare “A CMOS Class-E Cascode Power Amplifier For GSM Application” International Journal Of Recent Technology And Engineering (IJRTE) ISSN: 2277-3878, Volume-3, Issue-2, May 2014.
2. Chakkor Saad And Baghouri Mostafa “ Comparative Performance Analysis Of Wireless Communication Protocols For Intelligent Sensors And Their Applications” (IJACSA) International Journal Of Advanced Computer Science And Applications, Vol. 5, No. 4, 2014.
3. D. Chowdhury Et Al., “A Fully Integrated Dual-Mode Highly Linear 2.4 Ghz CMOS Power Amplifier For 4G Wimax Applications,” IEEE J. Solid-State Circuits, Vol. 44, No. 12, Pp. 3393-3402, Dec. 2009.
4. H. Yuan Lion “High-Linearity CMOS Feed Forward Power Amplifier For Wimax Application” 978-1-4244-3/08/$25.00, 2008 IEEE.
5. C. P. A. S. H. Ki Yong Son, “A 1.8-Ghz CMOS Power Amplifier Using Stacked Nmos And Pmos Structures For High-Voltage Operation,” IEEE Trans Micro. Theory Tech., Vol. 57, No. 11, Pp. 2652-2660, Nov. 2009.
6. M.Vasić And O. García, High Efficiency Power Amplifier For High Frequency Radio Transmitters, 978-1-4244-1/10/$25.00, 2010 IEEE.

AUTONOMOUS BASED PATH NAVIGATION FOR ROBOT USING MATLAB ADAPTIVE FUZZY LOGIC CONTROLLER

G. Archana[1]., C. Shanthi[2]., Ch. Mamatha[3]

1 Associate Professor, Department of ECE., CMR Institute of Technology., Kandlakoya Village.,
Medchal., TS, India (✉:- archana@gmail.com)
2 Associate Professor, Department of ECE., Malla Reddy Institute of Engineering & Technology., Maisammaguda.,
3 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— With the robot navigation method, a robot is driven to a certain position, the target, in an unknown environment without colliding. Here we offer a robotic navigation approach to dynamic environments with static and moving obstacles. The navigation method includes a static navigation method and dynamic route planning. Static navigation drives the robot to avoid static obstacles through the use of a fuzzy logic controller that includes four input and two output variables. When the robot detects moving obstacles, the robot can detect the speed and direction of movement of each obstacle and generate the corresponding flight path prediction table to predict the future flight path of the obstacles. If the table shows that the robot encounters an obstacle, dynamic route planning will find a new route to avoid the obstacle using the stopping strategy or the detour strategy.

Keywords— Fuzzy logic controller, Matlab, Path Navigation.

1. INTRODUCTION

A robot is a programmable machine that can use various types of sensors or web cams to extract information from its environment to plan and execute a collision-free path, avoiding the obstacle in front of the robot in its vicinity without human intervention. Navigation is a crucial issue for robots. A navigation system can be divided into two levels: high-level global planning and low-level reactive / local control. When planning at a high level, prior knowledge of the environment is available and the working area of the robot is fully or partially known. Using the world model, the global planner can determine the direction of movement of the robot and, in the case of complex obstacles, generate shorter paths to the destination. Therefore, it reacts quickly to unforeseen obstacles and uncertainties when the direction of movement is changed [3] .6

Fuzzy control systems are rule-based or knowledge-based systems that contain a number of IF-THEN fuzzy rules based on domain knowledge or human experts [6]. The simplicity of systems based on fuzzy rules and the ability to perform a wide variety of tasks without explicit calculations and measurements make it very popular with scientists and researchers.

2. SYSTEM DESCRIPTION

2.1 Design of a fuzzy controller

The schematic diagram of the fuzzy control is shown in FIG. The design steps for fuzzy controllers include: 1) initialization, 2) fuzzification, 3) inference, and 4) defuzzification.

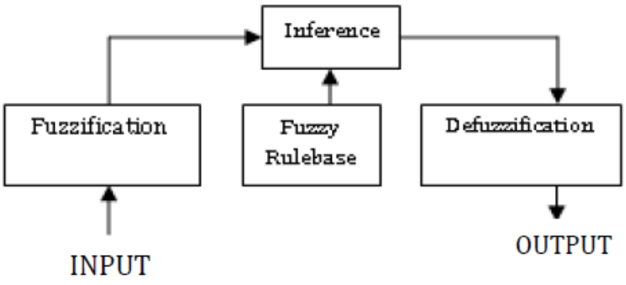


Fig. 1: The fuzzy structure of the controller

The first step is to identify the linguistic input and output variables and the definition of fuzzy sets (initialization). In fuzzy or fuzzy classification, a set of sharp data is converted into a set of fuzzy variables using membership functions (fuzzy sets).

3. DESCRIPTION OF THE PROPOSED SYSTEM

3.1 Function plan of the route navigation system

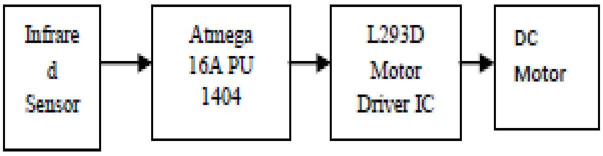


Fig. 2: Schematic representation of the route

The fuzzy rule base was burned into the microcontroller after being scrambled. The distances VERY NEAR, CLOSED and FAR to obstacles are considered as 3 digital threshold values in the digital domain for programming purposes. After the processing is done by the microcontroller for the logic of the given code, the required output pins (PORT B) connected to the motor control circuit L293D are activated. To drive the DC motors from the microcontroller, a motor interface card is being developed using L298D integrated circuit chips.

The motor control circuit moves the robot wheels forwards or backwards depending on the polarity of the voltages at their 4 outputs. Two DC motors independently control two wheels on a common axle. Two swivel castors are provided for support.

3.2 Circuit diagram

Fig 3 shows a circuit diagram for a route navigation based on fuzzy logic for a robot. In this route navigation robot, we used an infrared sensor to sense the obstacles in front of the robot and a comparator IC to compare the voltages. The comparator set in the non-inverting mode and the 10K potentiometer are connected to its inverting terminal to set the reference voltage, and the infrared receiver is connected directly to the non-inverting pins of the comparator. A red LED is connected to the output of on the sensor board.

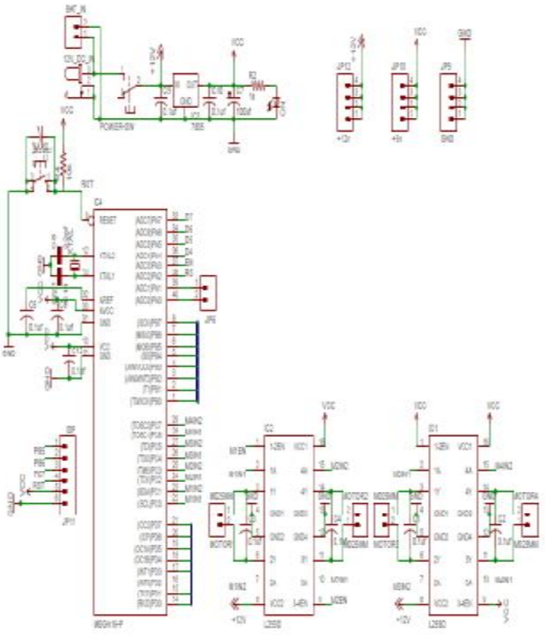


Fig. 3: Circuit diagram of the route navigation system

If this LED is blinking, it means our sensor is working. Then the signal goes to the Atmega16A PU microcontroller IC which is programmed and outputs the motor driver IC l293d which it has a basic function of increasing the voltage and current required to run the DC motor. Then the motor IC L293D rotates the motor according to the programming of the microcontroller IC. Therefore, the motor control IC is responsible for the movement of the wheels; H. Forward, left, right [1] [2].

4. RESULTS AND DISCUSSION

4.1 FUZZY INPUT AND OUTPUT ASSEMBLIES

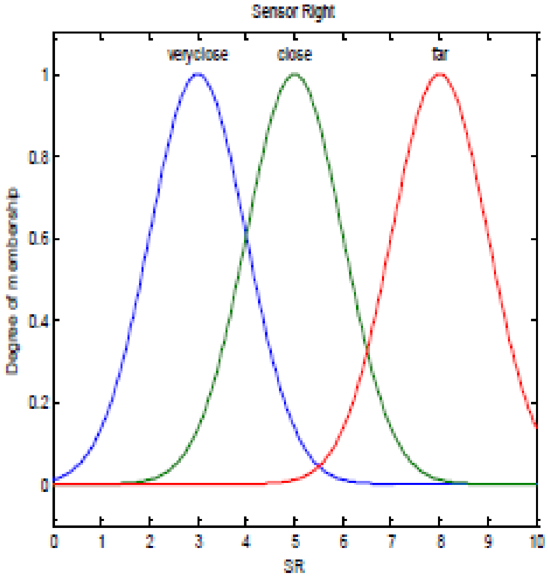


Fig. 4: Definition of the fuzzy set for the right input variable sensor

There are three inputs for the fuzzy logic system and one output. The inputs are essentially the right sensor (Fig. 4), the right sensor (Fig. 5) and the left sensor (Fig. 6). The exit is the direction (Fig. -7). This particular set of sentences is also spaced in the 0-10 input range. The vertical axis of this graph is the membership level, which ranges from 0 to 1. Depending on the input, the robot changes direction.

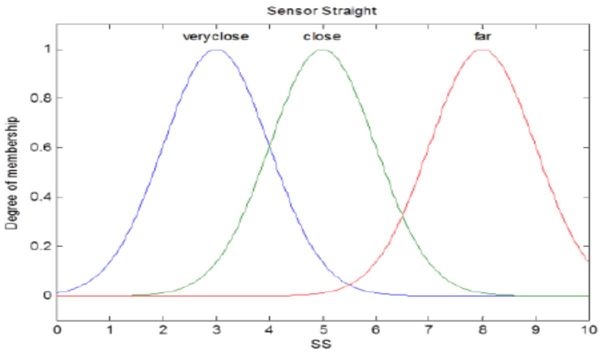


Fig. 5: Definition of the fuzzy set for a variable sensor with a right input

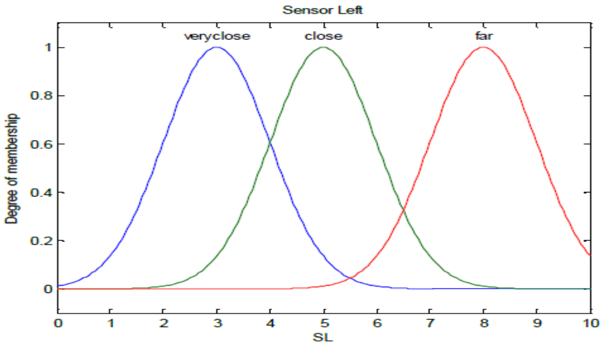


Fig. 6: Fuzzy set definition for the left input variable sensor

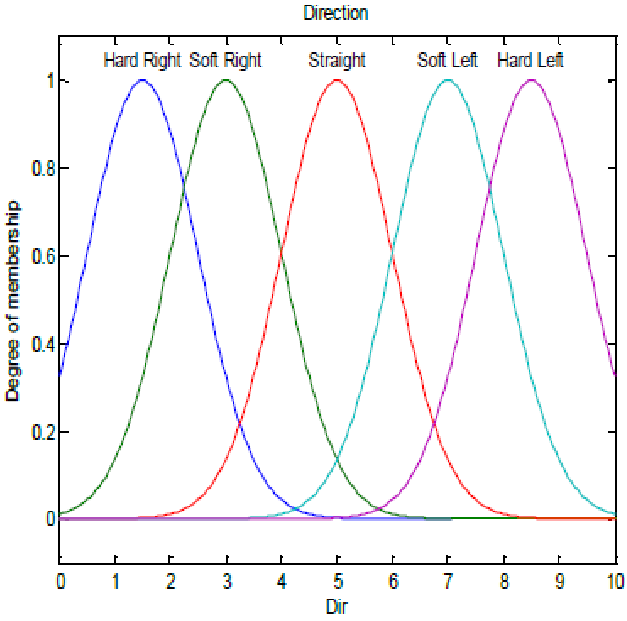


Fig. 7: Definition of the fuzzy set for the direction of the output variables

4.2 simulation results

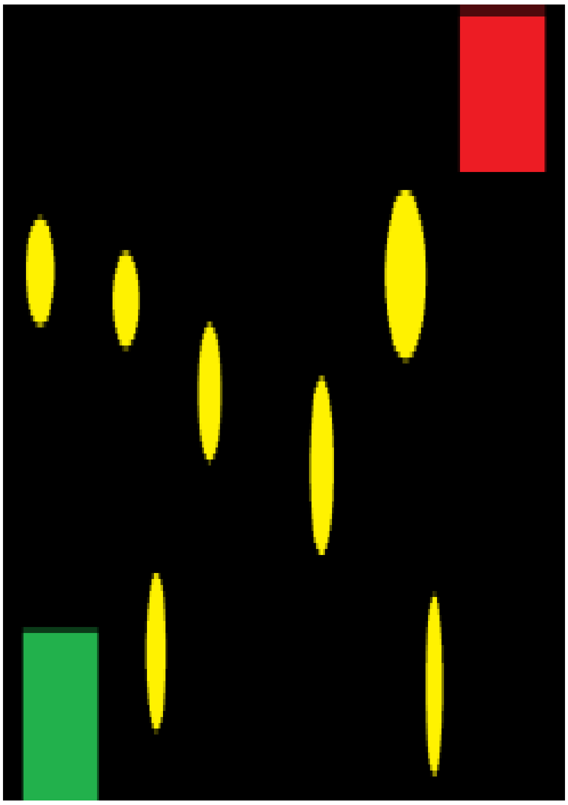
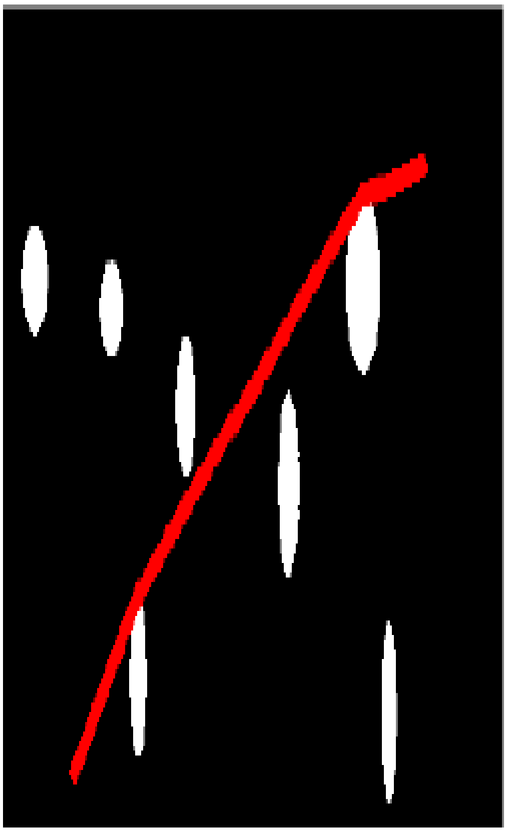


Fig. 8: Environment of the robot simulator

The path tracking control is tested with different robot starting and ending positions indoors. The controller first aligns the robot perpendicular to the desired path and then minimizes the distance to follow the path. Several navigation experiments were performed in an arena with yellow obstacles (detected by the sensor) and a red box representing the destination that the robot must reach, as shown in Fig. 8. Figure 9 shows the robot's steps to follow the path in a straight line.

Fig. 9: Robot is moving towards the target



5. CONCLUSIONS

The review of various works has shown that fuzzy logic control is one of the most successful techniques in designing and coordinating behavior for the navigation of mobile robots. In this chapter we first conduct a study to describe how fuzzy logic can be used to easily design individual behaviors and solve complex tasks by combining elementary behaviors [9]. Fuzzy control discussed a useful mechanism for designing various behaviors using linguistic rules. It also provided a robust methodology for behavior adjustment and arbitrage. Then two fuzzy controllers, which are supposed to demonstrate the influence and robustness of fuzzy control in a navigation system. The results obtained showed the correct functioning and efficiency of the fuzzy control for generating fluid movements, for shortening navigation time and for increasing robot safety [10]. In general, the advantages of fuzzy control when designing a navigation system are: i) ability to deal with uncertain and inaccurate information, ii) real-time operation, iii) easy combination and coordination of different behaviors, iv) ability to develop the perception of action-based strategies, and v) easy implementation.

6. FUTURE SCOPE

The work carried out as part of the project underscores the importance of the behavior-based model of robot navigation as an important path for the future of autonomous robotics. The work done in this project to make an obstacle avoidance robot would not have been possible with the traditional method. Therefore, the next day we will see more and more applications of fuzzy models of robot controls that are less dependent on the quality of the sensors, can handle noisy data, are open to the integration of new functions, are inherently robust and, above all, robust It has been found that in most cases they make the right choice when tested against the traditional very small robot. This work is extended to multiple robots rather than a single robot.

REFERENCES

1. N. T. Thanh and N. V. Afzulpurkar, “Dynamic path planning for a mobile robot using image processing,” Journal of Computer Science and Cybernectics, vol. 24, no. 4, pp.358-373, 2008.
2. P. Raja and S. Pugazhenthi, “Path planning for a mobile robot in dynamic environments, ”International Journal of the Physical Sciences, vol. 6, no. 20, pp. 4721-4731, 2011.
3. M. Faisal, K. Al-Mutib, R. Hedjar, H. Mathkour, M. Alsulaiman, and E. Mattar, “Multi modules fuzzy logic for mobile robots navigation and obstacle avoidance in unknown indoor dynamic environment,” in Proceedings of 2013 International Conference on Systems, Control and Informatics, pp. 371-379, 2013.
4. M. K. Singh, D. R. Parhi, S. Bhowmik, and S. K. Kashyap, “Intelligent controller for mobile robot: Fuzzy logic approach,” in Proceedings of 12th International Conference of International Association for Computer Methods and Advances in Geomechanics, pp. 1-6, 2008.
5. A.Fatmi, A. A. Yahmadi, L. Khriji, and N. Masmoudi, "A fuzzy logic based navigation of a mobile robot," in 22nd World Academy of Science, Engineering and Technology, 2006, pp. 169-174.

6. D. R. Parhi "Navigation of mobile robot using a fuzzy logic controller", J. Intell. Robot. Syst., vol. 42, no. 35, pp.253 - 273 2005.

EFFICIENT FILTER DESIGN FOR ACTIVE NOISE CONTROL SYSTEM USING MATRIX MULTIPLIER AND THE VEDIC MULTIPLIER

G. Kumar Swamy[1]., Mr. D. Gopi[2]., K. Sayanna[3]

1 Assistant Professor, Department of ECE., CMR Institute of Technology., Kandlakoya Village., Medchal., TS, India (✉:- kumarswamy@gmail.com)

2 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,

3 Associate Professor, Department of ECE., Anurag College of Engineering (ACE)., Ranga Reddy., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— Active Noise Control (ANC) is a method of noise cancellation in many applications such as industries, automobiles, household appliances, etc. The system consists mainly of an adaptive filter section and is implemented by a number of adders and multipliers. In this work different adders and multipliers are compared and those that are optimized for speed and surface efficiency are selected. In the proposed system, conventional adders and multipliers are replaced by highly zone-efficient spanning tree adders and modified Vedic multipliers. The comparison of the proposed system with the existing system shows a hardware efficiency of 4.8% and a time reduction of 40.41%. The system simulation is validated on Xilinx 14.2 ISE and synthesized on Xilinx Virtex-5 FPGA

***Keywords*— Active Noise Control, Vedic multipliers, Parallel Prefix Adders and Xilinx.**

1. INTRODUCTION

Active Noise Control (ANC) is a method of removing audio noise. This system uses a number of secondary sources to create an anti-noise wave that cancels out the noise wave. The noise suppression signal is a wave with the same amplitude and phase as the noise signal. ANC works on the principle of superposition. The noise suppression signal is made to overlap the noise signal and they are effectively cancelled and a noise-free output is obtained. The secondary sources are connected by a suitable signal processing algorithm. Many applications find use for ANC, e.g. B. in industries, automobiles, etc.

2. EXISTING SYSTEM

Active Noise Control (ANC) uses an electro acoustic system to suppress primary noise based on the principle of layering. The main part of the system is a filter section for extracting the signal. The input to the filter is a noisy signal. The output filter may be wrong due to noise. The output of the filter is subtracted from the desired signal to obtain the error signal. The filter weights are updated according to the signal. A noise suppression signal is generated to combine with the output of the filter to obtain the error free signal. The main part of the system are adders and an adaptive filter section.

3. PROPOSED SYSTEM

Adaptive filters are linear filters with the ability to update filter weights according to a specific optimization algorithm. It consists of a filter section (IIR / FIR) and a weight enhancement part. The basic circuit of an adaptive filter is shown in Figure -2. The filter usually gives the convolution of the input and the weights as output y (n). The aim is to bring y (n) closer to the desired signal d (n). If "n" changes, the system adjusts the weights to get y (n) an estimate close to d (n).

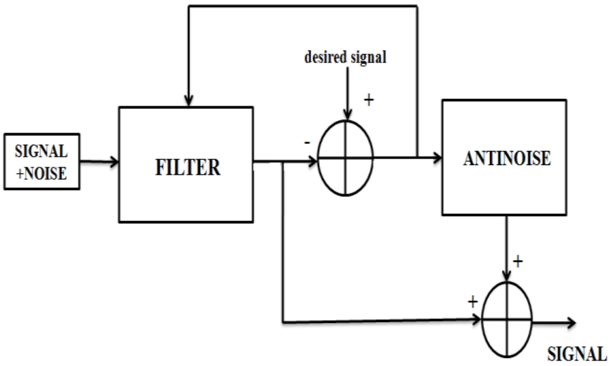


Fig. 1: Functional diagram of the conventional system

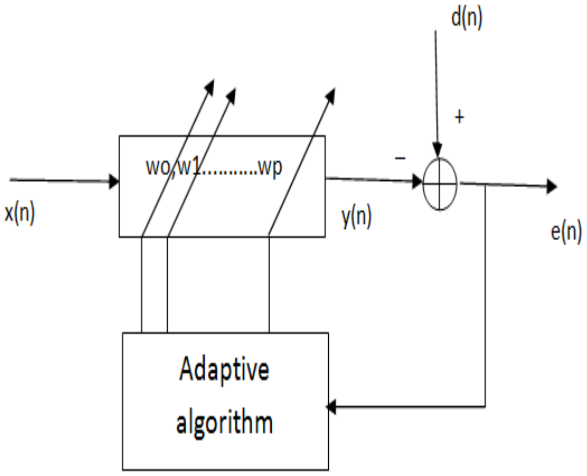


Fig. 2: Adaptive filter circuit

In the filter section, a controller supplies the necessary control signals and addresses to the memory buffers. It consists of two counters that can count from 0 to M-1, where M is the length of the filter. Here the filter length is assumed to be 24. Therefore the counters count from 0 to 23. A comparator is included to switch off the counting of a cycle so that the new value can be saved every 24 cycles. The hardware of the control circuit is shown in Fig. -3.

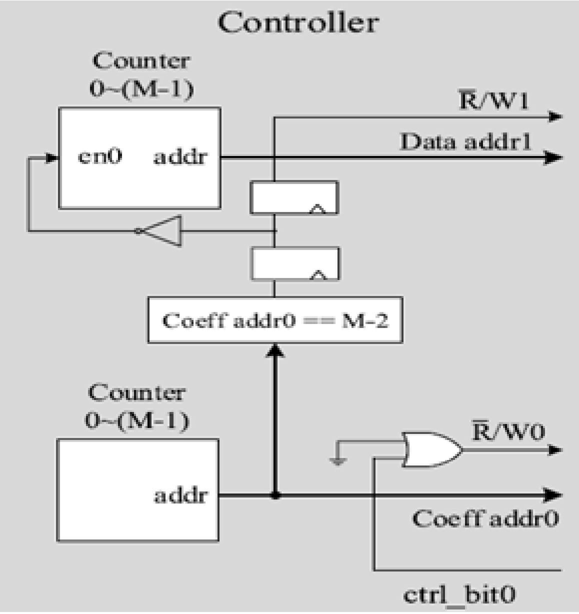


Fig - 3: Control circuit [1]

The filter weights are updated depending on the situation. The new weights are calculated using the following equation:

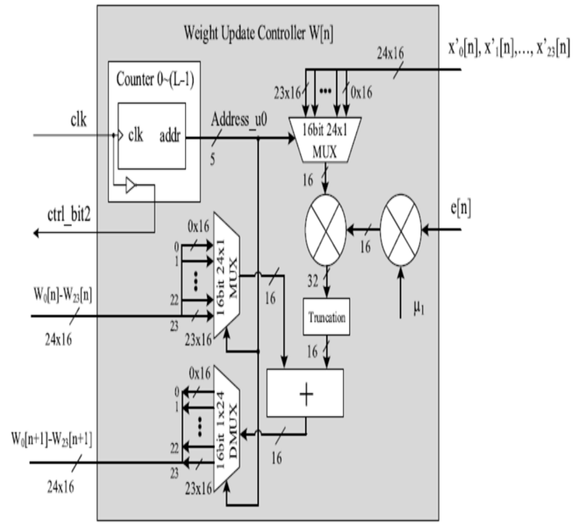


Fig. 4: Weight update block [1]

System-wide adders are replaced by a spanning tree adder. The spanning shaft adder is a type of parallel prefix adder (PPA) that has been used to improve area, delay and energy efficiency [3]. The two main elements of a parallel prefix adder are black cells (BC) and gray cells (GC). The number of steps for generating the carry signal is reduced with PPAs compared to CLA. In PPAs, the delay is logarithmically proportional to the width of the adder.

4. RESULTS AND DISCUSSION

The system was developed with the Xilinx ISE 14.2 Design Suite and implemented on the Spartan-3E FPGA Basys2 card. The result of the simulation, the RTL, the graph, the summary of the use of the device and the energy consumed by the system are covered in this section.

The matrix multiplier and the Vedic multiplier were compared and the results obtained. The comparison is shown in Figure -1. The number of wafer, IOB, and slice LUTs was significantly reduced, resulting in an overall reduction in area. The system lag has also been reduced. It can be seen from the diagram that a surface efficiency of 89.2% and a delay reduction of 79.6% were obtained for the multiplier module.

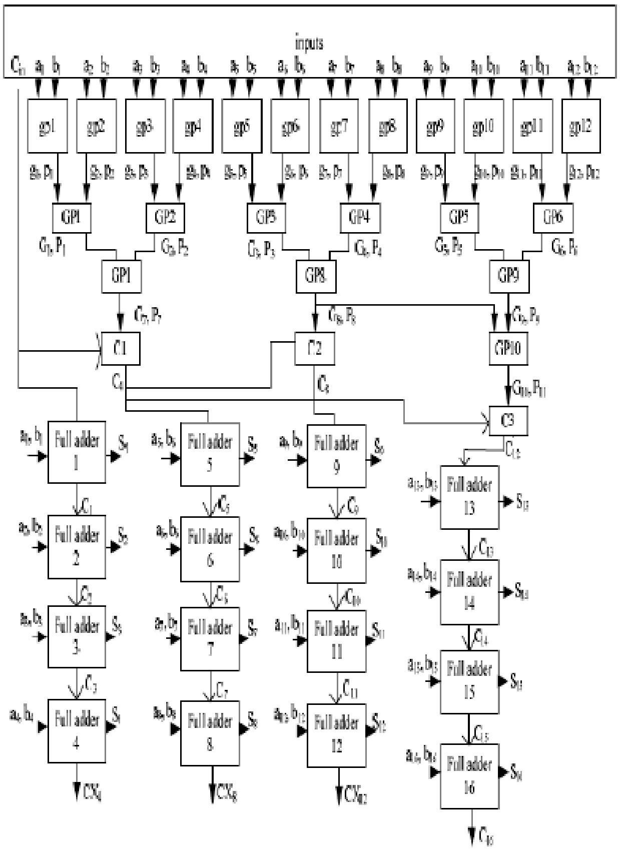


Fig - 5: Cross wave adder [3]

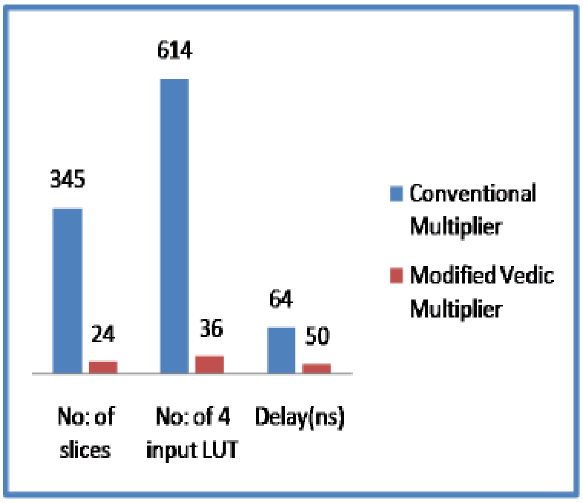


Fig 6: Comparison of area and lag multipliers.

A comparison was made between four parallel 16-bit prefix adders (Koggestone adder, Brent Kung adder, sparse Koggestone adder, and Spanning Tree adder) with a 16-bit CLA. All parallel prefix adders use less area than CLA, but spanning tree adders show both area and delay optimization. STA has an area efficiency of 16.5% and a delay reduction of 21%.

The conventional ANC system and the modified system were compared and the results are shown in Table -1. The number of cutoff LUTs has been reduced from 746 to 710, which shows an improvement in the area. In addition, in the event of a delay, there is a large reduction from 22,382 ns to 13,337 ns.

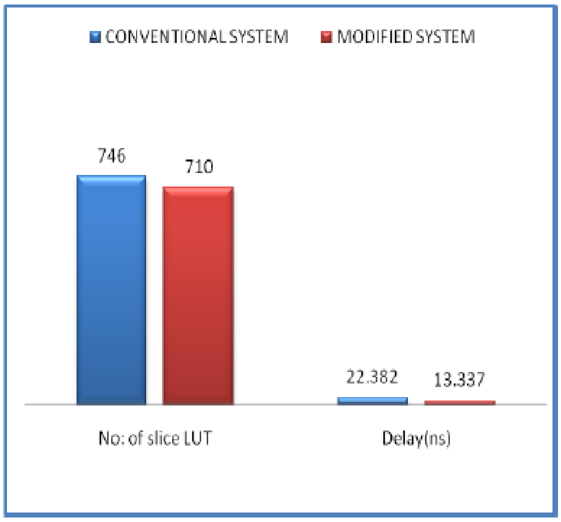


Fig 7: Comparison of conventional and modified ANC systems.

5. CONCLUSIONS

Active noise reduction is a method of noise cancellation. An efficient filter has been proposed for the active noise control system. The system's multipliers and adders are being replaced by modified high-speed Vedic multipliers and spanning tree adders. Various parallel prefix adders have been explored and finally spanning tree adders are chosen for their efficiency. A comparison of the conventional and the proposed active noise control system is made. You get 4.8% hardware efficiency and a 40.41% lead time reduction.

REFERENCES

1. X. Kong and S. M. Kuo, “Study of causality constraint on feedforward active noise control systems,” IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process., vol. 46, no. 2, pp. 183–186, Feb. 1999.
2. Y. Song, Y. Gong, and S. M. Kuo, “A robust hybrid feedback active noise cancellation headset,” IEEE Trans. Speech Audio Process., vol. 13, no. 4, pp. 607–617, Jul. 2005.
3. S. M. Kuo, S. Mitra, and W.-S. Gan, “Active noise control system for headphone applications,” IEEE Trans. Control Syst. Technol., vol. 14, no. 2, pp. 331–335, Mar. 2006.
4. Sudheer Kumar Yezerla and B Rajendra Naik,“Design and Estimation of delay, power and area for Parallel prefix adders”, in Proceedings of 2014 RAECS UIET Punjab University Chandigarh, 06 - 08 March, 2014.
5. S. M. Kuo and D. R. Morgan, “Active noise control: A tutorial review,”Proc. IEEE, vol. 87, no. 6, pp. 943–973, Jun. 1999.
6. K.-K. Shyu, C.-Y. Ho, and C.-Y. Chang, “A study on using microcontroller to design active noise control systems,” in Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS), Nov. 2014, pp. 443–446.
7. Hong-Son Vu and Kuan-Hung Chen, “A Low-Power Broad-Bandwidth Noise Cancellation VLSI Circuit Design for In-Ear Headphones.”, IEEE Trans. Very Large Scale Integration (VLSI) Systems, vol. 24, no. 6, pp. 2013-2025, June 2016.
8. Udit Narula, Rajan Tripathi and Garima Wakhle,“High Speed 16-bit Digital Vedic Multiplier using FPGA ” in 2nd International Conference on Computing for Sustainable Global Development ,2015,pp. 121-124.
9. Douglas S.C, Introduction to Adaptive Filters, Digital Signal Processing Handbook., CRC Press LLC, 1999.

DESIGN OF LOW-POWER CONFIGURABLE VITERBI DECODER IN VLSI ARCHITECTURE

Sk. Neelofer[1]., R. Sahithi[2]., J. Srinu[3]

1 Assistant Professor, Department of ECE., CMR Institute of Technology., Kandlakoya Village, Medchal Rd., Medchal., TS, India (✉:- neelofer@gmail.com)

2 Assistant Professor, Department of ECE., CMR College of Engineering & Technology - [CMRCET]., Hyderabad.,
3 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— ***The convolutional coding and the Viterbi algorithm are fundamental concepts of the error correction method. The Viterbi algorithm is one of the decoding methods for correcting data errors. In VLSI, design challenges are often related to performance, surface area, speed, complexity, and configurability. This article proposed a configurable, low power design for a Viterbi decoder for hard decisions in VLSI. For each trace number, the layout can be configured by increasing or decreasing the size of the trace parameters. It takes N + 2 clock cycles of latency to complete the process, where N is the tracking number. In this study, configuration tests were performed for N = 32 and N = 64. The design was also synthesized on Xilinx as target plaques. It delivers good synthesis results in terms of operating speed and surface area consumption.***

Keywords— ***Viterbi decoder, convolutional encoder, low power consumption, VLSI.***

1. INTRODUCTION

Many methods have been proposed in the field of error correction. One of the most popular methods is the Viterbi algorithm. The comprehensive error correction method consists of three main parts: convolutional coding, error disturbance, and Viterbi decoding. The original data becomes complicated by using its specific convolution formula to generate a code word. Each code word consists of 2 bits. The key word is the representation of the two original data and their redundant ones. Therefore, when data transmission errors occur, we can reconstruct the correct data using the Viterbi algorithm.

Habib et al. [1] discussed exploring the design space in viterbi's hard decision algorithm and its VLSI implementation. Jinjin He et al. [2] have proposed a high speed, low performance Viterbi decoder that uses the T algorithm as the precomputation architecture for the Trellis Coded Modulation (TCM) system. The problem of low power consumption is important because the Viterbi decoder is a very power-consuming module in the TCM [3]. In relation to this question, Chakraborty et al. [4] also proposed a design to reduce power consumption in the Viterbi decoder. Another problem is the speed of operation. Jinjin He et al. And Azhar et al. Discussed how to increase the operating speed of the Viterbi decoder.

2. SYSTEM DESIGN

Convolutional codes are sometimes referred to as lattice codes. Convolutional coding is easy, but decoding is much more difficult. Convolutional codes
are generally characterized by two parameters and models of n modulo 2 adders. The two most important parameters are the code rate and the length of the restriction. The code rate is the number of bits transmitted per input bit, for example a 1/2 code rate, and generates 2 bits for transmission.

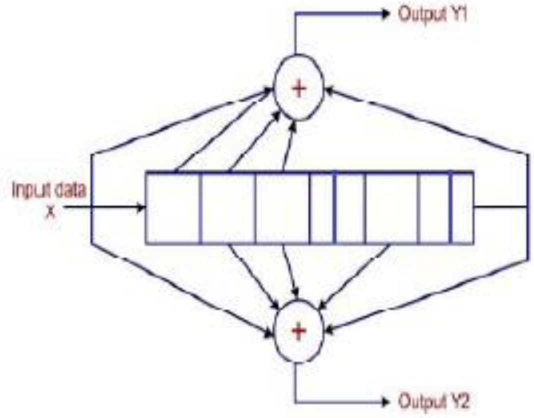


Figure 1: Convolutional encoder with the constraint length k = 9

Convolutional codes are sometimes referred to as lattice codes. Convolutional coding is easy, but decoding is much more difficult. Convolutional codes are generally characterized by two parameters and models of n modulo 2 adders. The two important parameters are the code rate and the length of the restriction. The code rate is the number of bits transmitted per input bit, for example a 1/2 code rate, and generates 2 bits for transmission.

The encoder has modulo-2 adders and n generator polynomials, one for each adder. An input bit m1 is applied to the leftmost register. Using the generator polynomials and the existing values in the remaining registers, the encoder generates n bits. As shown in Figure 1, we have a general encoder with a code rate (k / n) of 1/2 and a sequence of information modified to record 1 bit at a time. The shift register has a constraint length (K) of 3 which corresponds to the number of stages in the register. The output of the encoder is referred to as a code symbol. During the initialization, all encoder levels are initially set to zero. The output of the encoder is determined by the polynomial equations of the generator. Since the complexity of the encoder increases exponentially with the restriction length, none of the encoders uses more than a restriction length of 9 for practical reasons [5].

3. VITERBI DECODER

The basic components of the Viterbi decoder are the branch metric unit (BMU), the path metric unit (PMU), the addition selection and comparison unit (ACSU) and the management unit. Survival Storage (SMU).

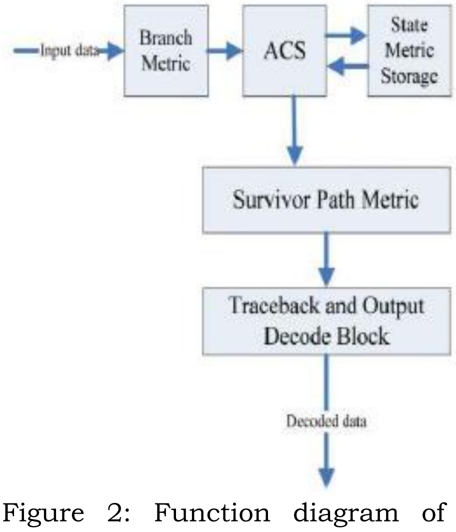


Figure 2: Function diagram of the Viterbi decoder

3.1 Metric Branch Unit (BMU)

The first unit is called the metric branch unit. Here the received data symbols are compared with the ideal encoder outputs of the transmitter and the branch metric is calculated. The Hamming distance or Euclidean distance is used to compute branch metrics.

3.2 Metric Street Unit

The second unit, referred to as the route metric calculation unit, calculates the route metrics for a leg by adding the branch metrics associated with a received symbol to the route metrics of the previous floor of the grid.

3.3 Add, Compare and Select Unit (ACSU)

The ACSU consists of 64 ACS units, each of which consists of an ACS butterfly module that adds the appropriate BM to the corresponding PM, compares the new PM, feeds the selected PM to the ACSU and generates the decision bits. The decoder implements adders to calculate the route metric and a comparison and selection section to decide which the best route is. Using the serial bit architecture can reduce the performance of the Viterbi decoder.

The two ACS processors that use the same inputs can be combined in a butterfly processor. There are 64 states, so 32 butterflies are required. Due to the butterfly structure, the connections are reduced due to the power reduction. The illustration shows the Radix 2 accelerator module. The inputs j and j + N / 2 are shared for the output jy 2j + 1.m There are two paths that reach each node. One is for transition 0 and another is for transition 1. If the input is 0 in the current state, the next state is 2j, but if the input is in the current state 1, the output is 2d + 1. It is affected. The branch metric and the route metric of the i-th route and the j-th route are cumulated. If the cumulative route metric of the i-th route is smaller, the decision is made in favor of the i-th route and the generated decision bit is 0. The new route metric is the cumulative route metric of the i-th route.

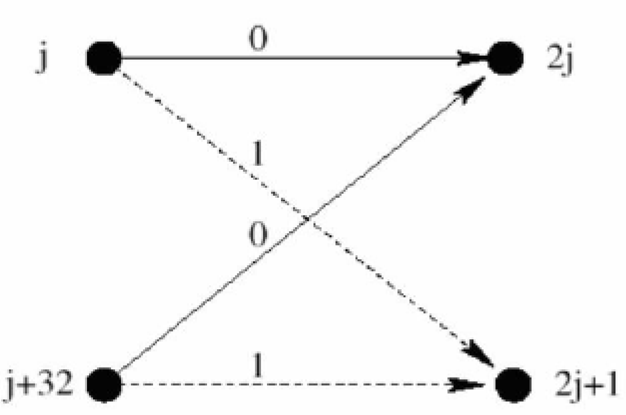


Figure 3: Radix 2 butterfly structure

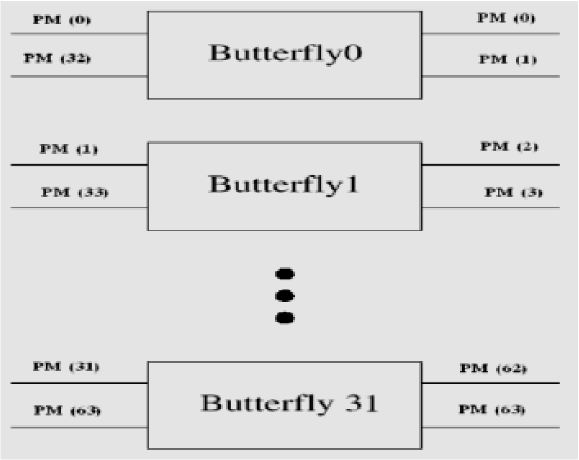


Figure 4: Connected ACS unit

4. RESULT ANALYSIS

In the TB method, the memory can be implemented as RAM and is called path memory. Compare in the ACS unit and do not store actual survivors. Once at least L branches have been processed, the network connections are retrieved in reverse order and the path is traced through the network diagram. Starting from the state with the minimum of PM, the TB method extracts the decoded bits.

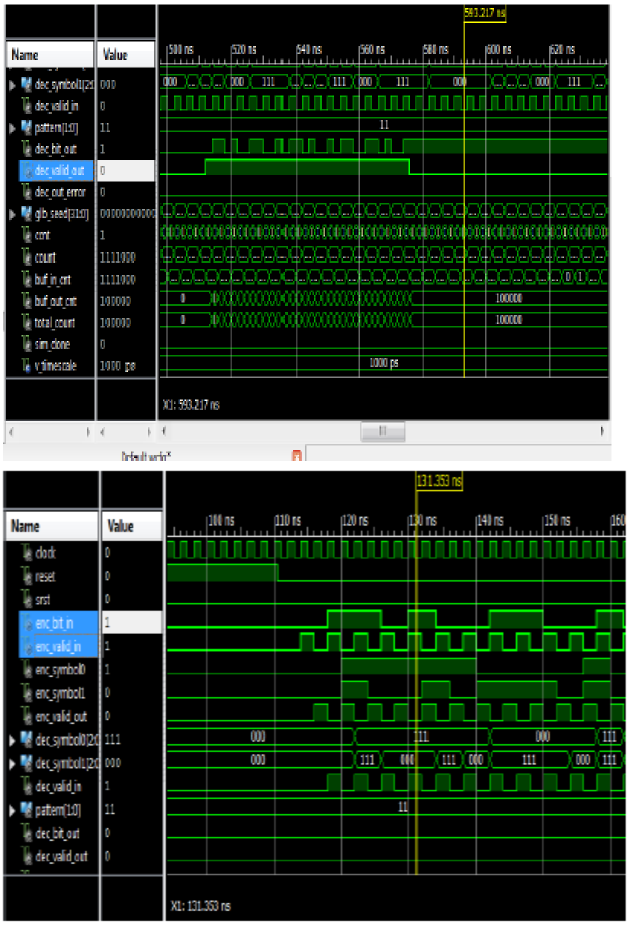


Figure 5: Simulation result for encoder and decoder

Based on this state and in the time following the survivor's path, a unique path is identified that originally contributed to the current MP. When drawing through the grid, the decoded output sequence is generated in reverse order [8], which corresponds to the branches drawn. The trace architecture limits the decoding speed [9], since the memory bandwidth is limited by nature.

5. CONCLUSION

This article proposed a configurable, low power design for a Viterbi decoder for hard decisions in VLSI. For each trace number, the layout can be configured by increasing or decreasing the size of the trace parameters. It takes N + 2 clock cycles of latency to complete the process, where N is the tracking number. In this study, configuration tests were performed for N = 32 and N = 64. The design was also synthesized on Xilinx as target plaques. It delivers good synthesis results in terms of operating speed and surface area consumption.

REFERENCES

1. "Design of a High-Throughput Low-Power IS95 Viterbi Decoder" Xun Liu Marios C. Papaefthymiou. Advanced Computer Architecture Laboratory, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, Michigan.
2. R.A.Abdallah, N.R.Shanbhag, "Error-resilient low-power viterbi decoder architectures", IEEE Trans. Signal Process., vol. 57, no. 12, pp. 4906-4917, Dec. 2009 Modulation Detection and Coding" Tommy Oberg (2001). Wiley and Sons. Pp 81- 86.
3. "VLSI Design and Implementation of High Speed Viterbi Decoder" WANG Jin-xiang, YOU Yu-xin, LAI Feng-chang and YE Yi-zheng (2002).
4. "A Convolutional Code Decoder Design Using Viterbi Algorithm with Register Exchange History Unit" Vasily P. Pribylov, Alexander I. Plyasunov (2005). SIBCON. IEEE.
5. "Efficient Scalable Architectures for Viterbi Decoders"Stefan Bitterlich and Heinrich Meyr (1993). Aachen University of Technology, Templergraben , Germany. pp 89-100.
6. K. Hasnain, and Azam Beg and "Performance Analysis of Viterbi Decoder Using a DSP Technique", 8th

IEEE International Multitopic Conference(ITMIC'04), Dec 2004,pp.201-207.

7. S. Ranpara, On a Viterbi Decoder Design for LowPower Dissipation, M.S. Thesis, Dept. of Electrical and Computer Eng., Virginia Polytechnic Institute and State University, April 1999.

DESIGN OF DIGITAL RECEIVER USING DIGITAL DOWN CONVERTER IN SPARTAN 6 FPGA

R. Raj Kumar[1]., Mr. Venkata Siva Reddy[2]., K. Vamshi[3]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., TS, India (✉: chunchurajkumar@gmail.com)

2 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,

3 Associate Professor, Department of ECE., CMR Institute of Technology., Kandlakoya Village., Medchal Rd., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— ***In the past, radio receivers were designed with analog circuitry, but to overcome the disadvantages of analog circuitry, everything is now digitized. Therefore, wireless communication is in great demand in today's world. The digital receiver must communicate with all new radio standards. Digital receivers are used to get RADAR information from target devices. In this proposed article, 70 MHz Doppler is sampled by a digital receiver and ADC of this analog signal at a high sampling frequency. The scanning technique used for this is band pass scanning, ie sub sampling. To minimize the sampling rate in digital, there is a digital down converter (DDC) that is used for frequency conversion and a better decimation factor. After this process, we got a more precise and stable signal and it is very easy to collect information about the target. The entire digital receiver architecture is implemented in Xilinx IP Core and captured in FPGA (Spartan 6 SP601), which is connected to ADC (LTC 2107) via an FMC connector.*** .

Keywords— Digital Receiver, ADC (DC2266A), Field Programmable Gate Array (FPGA), Spartan 6 SP601, Digital Clock Manager (DCM), Digital down converter, Digital filter.

1. INTRODUCTION

In order to overcome the disadvantages of analog receivers such as low interference immunity, aging of the components, temperature drift, calibration, requirement of specific H / W and S / W values, etc., the digital receiver entered the scene. This project focuses on the design and implementation of a digital receiver using FPGA. The main components of the receiver are the anti-aliasing filter to remove the aliasing effect, the high-speed A / D converter (LTC2107) from Linear Technology, and an ADC controller (LTC6409) from Linear Technology, which is sampled using the scan Bandpass, the output of which is then sent to the mixer that performs the frequency conversion and supplied to the decimator low-pass filter, which converts the signal to the I and Q format assigned to a surveillance system via Ethernet, and can several parameters CLOUD RADAR. DF is an ideal application for digital receivers because of its excellent channel-to-channel channel matching and constant delay characteristics. Radar applications benefit from the close coupling of A / D, digital receiver and DSP functions for processing broadband signals. FPGAs are particularly well suited for the FFT and pulse compression tasks normally required in signal processing sections.

2. DESCRIPTION AND THEORY OF THE SYSTEM

Looking at the general block diagram, the digital samples coming from the A / D converter are sent to the next stage, the digital receiver chip, on the red line, as shown in Figure 1. The digital receiver chip is usually contained in a single monolithic chip that forms the heart of the digital receiver system. It is also sometimes referred to as a digital down converter (DDC) or digital down receiver (DDR) [2].

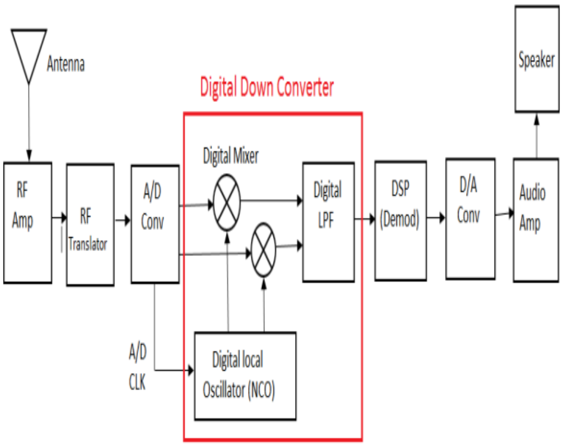


Fig. -1: Function diagram of the digital receiver

There are three main sections within the digital buck converter:

- Local oscillator
- Digital mixer
- Decimating low pass filter

The oscillator is generated with a sampling rate that corresponds exactly to the A / D sampling clock rate fs 60 MSPS. The next main component of the digital receiver chip is the mixer, which consists of two digital multipliers. Once the RF signal is translated, it can be filtered. The decimating low pass filter accepts input samples from the mixer output at the full A / D sampling rate fs. It uses digital signal processing to implement a Finite Impulse Response (FIR) filter transfer function.

3. DIGITAL RECEIVER

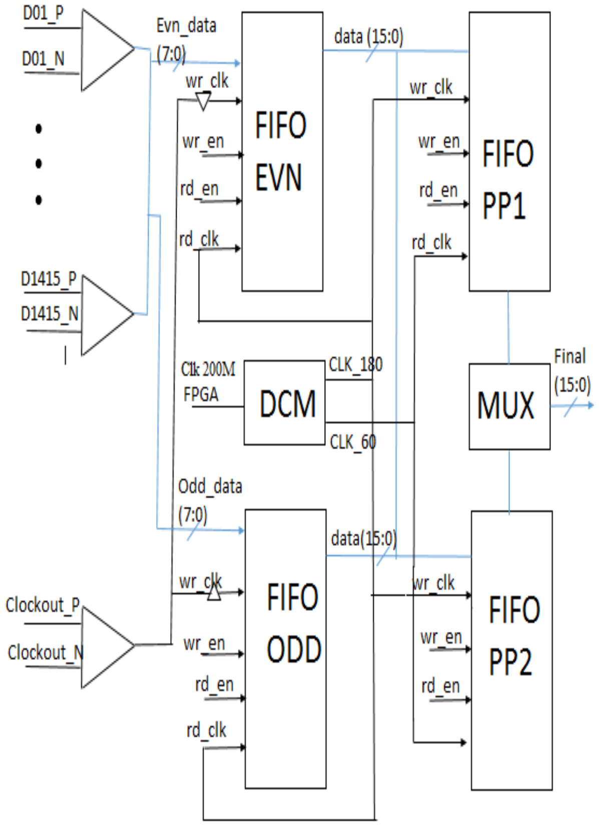


Fig. -2: Acquire digital signals from the CAN

In Figure 3, the analog input is controlled by an ADC controller (LTC6409), which converts the unbalanced input into a differential output, which is then fed into the ADC (LTC2107) and gives the output a digital 16-bit LVDS signal [3].

In the two-rate LVDS mode, two data bits are multiplexed and output at each differential output pair. There are eight pairs of LVDSADC data outputs (D01 + / D01 to D1415 + / D1415). The overflow (OF + / OF) and the data output clock (CLKOUT + / CLKOUT) each have an LVDS output pair. Digital outputs with double data rate Two data bits are multiplexed into each differential output pair.

3.1 Bandpass Sampling

Although it satisfies most sampling needs, the sampling of low pass signals is not the only sampling scheme used in practice. We can use a technique known as bandpass sampling to sample a continuous bandpass signal that is centered on a frequency other than zero Hz. The acceptable frequency range for bandpass scanning can be calculated using the following formula.

$$\frac{2Fc - BW}{M} \geq fs \geq \frac{2Fc + BW}{M + 1}$$

4. HARDWARE CONFIGURATION

The ADC evaluation board is connected to the FPGA SP601 via the FMC-LPC connector. The FPGA Mezzanine Card (FMC) is an ANSI / VITA standard that defines intermediate I / O modules for connection to an FPGA or other device with reconfigurable I / O capability. It has a low-profile connector and a compact card size for compatibility with various industry-standard form factors of slot cards, blades, low-profile motherboards, and mezzanines.

Fig. -3: Hardware configuration

3.4 Digital Clock Manager (DCM)

The Clock Wizard helps to create the clock circuit for the required output clock frequency, phase and duty cycle using the mixed clock management primitive (MMCM) or the phase locked loop (PLL).

4. RESULTS AND DISCUSSIONS

4.1 Programming the ADC with SPI

After connecting the ADC to the FPGA via the FMC-LPC connector, the SPI protocol is used to transfer data and configure the ADC register.

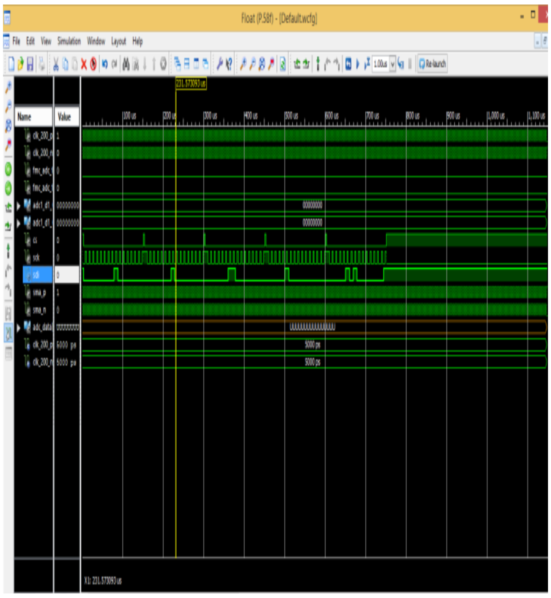

Float (P.58f) - [Default.wcfg]
File Edit View Simulation Window Layout Help
Name
Value

Fig. -4: VHDL output for programming the ADC

The SS, SCLK, MISO, and MOSI pins become a serial interface that programs the ADC mode control registers. Data transmission starts when SS drops out. Data is written to a register with a 16-bit serial word. Data on the MOSI pin is buffered on the first 16 rising edges of SCLK. Data transmission ends when SS ascends.

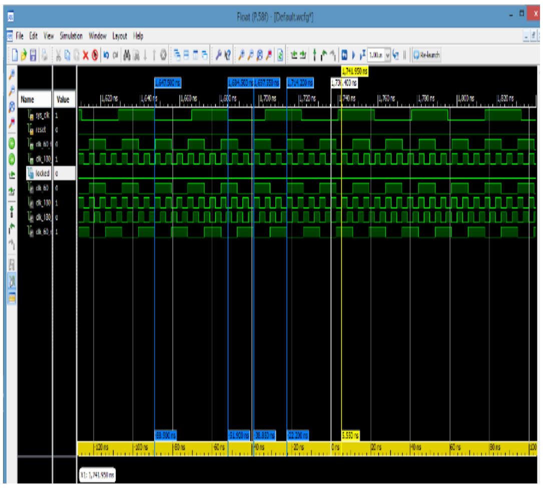
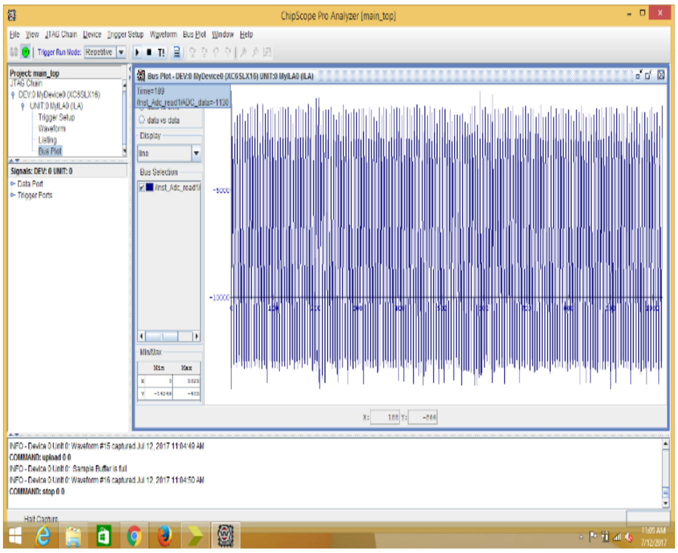

Float (P.58f) - [Default.wcfg]
File Edit View Simulation Window Layout Help
Name
Value

Fig. -5: VHDL output from DCM

4.3 Acquired ADC output

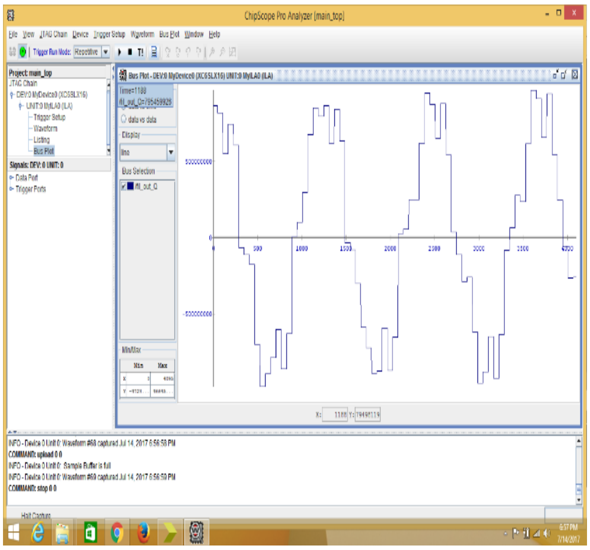
The final data output from 16-bit ping-pong FIFOs can be read with a 60 MHz clock. The output is displayed in the ISE 4.7 Design Suite's Chip Scope software. The ADC output data comes from the rising and falling edges of CLKOUT + with a frequency of 60 MHz. The ADC input is 70 MHz with Doppler (intermediate frequency) and is sampled at a sampling rate of 60 MSPS.


ChipScope Pro Analyzer [main_top]
File View JTAG Chain Device Trigger Setup Waveform Bus Plot Window Help
Trigger Run Mode: Repetitive
Project: main_top
JTAG Chain
DEV:0 MyDevice0 (XC6SLX16)
UNIT:0 MyILA0 (ILA)
Trigger Setup
Waveform
Listing
Bus Plot
Signals: DEV:0 UNIT:0
Data Port
Trigger Ports
Bus Plot - DEV:0 MyDevice0 (XC6SLX16) UNIT:0 MyILA0 (ILA)
data vs data
Display
line
Bus Selection
Min/Max
Min
Max
X
Y
Halt Capture

```
INFO - Device 0 Unit 0: Waveform #15 captured Jul 12, 2017 11:04:49 AM
COMMAND: upload 0 0
INFO - Device 0 Unit 0:  Sample Buffer is full
INFO - Device 0 Unit 0: Waveform #16 captured Jul 12, 2017 11:04:50 AM
COMMAND: stop 0 0
```

Fig. -6: ADC data recorded 10.3 MHz at 60 MSPS

The post-processing of this signal is decimated. Signals via I and Q have a sample rate of 60 MSPS, so the system configuration requires a sample rate of 1 MSPS. So if you collect 1 in 60 samples, the result is a sample rate of 1 MSPS. The following figure shows the signal of a 500 kHz signal with a sampling rate of 1 MSPS.


ChipScope Pro Analyzer [main_top]
File View JTAG Chain Device Trigger Setup Waveform Bus Plot Window Help
Trigger Run Mode: Repetitive
Project: main_top
JTAG Chain
DEV:0 MyDevice0 (XC6SLX16)
UNIT:0 MyILA0 (ILA)
Trigger Setup
Waveform
Listing
Bus Plot
Signals: DEV:0 UNIT:0
Data Port
Trigger Ports
Bus Plot - DEV:0 MyDevice0 (XC6SLX16) UNIT:0 MyILA0 (ILA)
data vs data
Display
line
Bus Selection
Min/Max
Min
Max
X
Y
X: 1188 Y: 79498119
Halt Capture

```
INFO - Device 0 Unit 0: Waveform #68 captured Jul 14, 2017 6:56:58 PM
COMMAND: upload 0 0
INFO - Device 0 Unit 0:  Sample Buffer is full
INFO - Device 0 Unit 0: Waveform #69 captured Jul 14, 2017 6:56:59 PM
COMMAND: stop 0 0
```

Fig. -7: Output decimated at 1 MSPS

5. CONCLUSION

The advantages of using a digital receiver are reduced DSP processing requirements, very fast tuning, no PLL, fast bandwidth selection, zero frequency deviation and error, precise filter characteristics and stable, excellent dynamic range, etc. The front ADC circuit design is complete and the final board is also tested by connecting it to the Spartan-6 (SP601) evaluation board via the FMC connector.

REFERENCES

1. Rodger H. Hosking,"Digital Receiver Handbook: Basics of Software Radio", Fifth Edition Pentek.
2. Doglas Perry, VHDL Programming by examples, 4th Edition, McGraw-Hill Professional, July 2002.
3. Linear Technology,"10GHz GBW, 1.1nV/p Hz Differential Amplifier/ADC Driver", LTC6409 datasheet, 2010.
4. Linear Technology,"16-Bit, 210Msps High Performance ADC", LTC2107 datasheet, 2014.
5. Richard G. Lyons, Understanding Digital Signal Processing, 3rd edition, Prentice, Hall, November 2010.
6. Dr. M. Kamaraju, Jayaraju. D, FPGA Based 70MHz Digital Receiver, for RADAR Applications, International Journal of Research in Electronics Communication Technology Volume 1, Issue 1, July-September, 2013, pp. 01-07.

"

REVIEW ON DATA TRANSMISSION AND RECEPTION THROUGH USB 2.0 TRANSCEIVER IN VHDL

D.Prasad[1]., V. Sreekanth Reddy[2]

1 Assistant Professor, Department of ECE., St. Martins Engineering College., Secunderabad.,

Secunderabad., TS, India (✉: prasad @gmail.com)

2 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The scope of the project is based on a USB controller which depends on the A / V host controller. High-speed data flowing between video and audio devices improves speed in phone, electronics integration applications, consumers, and productivity. USB is designed for the standardized connection of computer applications. Data storage dangerous, the transport of personal data makes sense. Universal Serial Bus is an industry standard that defines cable connectors and communication protocols for the connection, communication, and power supply between computers and electronic devices. As usual, the architecture of the USB receiver / transmitter is innovative in this approach. The various concepts were implemented in a hardware description language in order to provide a model for the simulations. At the same time, the code can be synthesized and physically implemented in programmable logic modules..

Keywords— USB, Computer Telephony Integration, transmitter, Receiver

1. INTRODUCTION

All communication via USB takes place from the host under software control. The host hardware consists of the USB host controller, which initiates transactions via the USB system, and the root hub, which provides connection points for the USB device. The host controller is responsible for generating the transactions scheduled by the host software. The host controller driver creates a linked list of in-memory data structures that define the transactions that should take place during a particular frame. These data structures, known as transfer descriptors, contain all of the information the host controller needs to generate transactions. The USB standard was developed to eliminate the shortcomings of the old interfaces for PC peripherals. The standard makes the interface to the PC extremely simple for the end user and more complicated life for the developer of peripheral devices. The USB 2.0 transceiver macro cell understands the USB protocol and can perform transactions on behalf of the device. Verilog is a hardware description language that is widely used in the VLSI industry.

2. EXISTING WORK

To test our project we will be using memory to store the descriptors to be transferred that are actually provided by the USB device driver. These descriptors are sent to the packet generation unit and then to the SIE which adds SYNC, EOP and CRC bits, does a bit fill and finally encodes it in NRZI format before being transmitted to the USB. Transmission and isochronous transmission. Control transfer as needed for a new device setup and isochronous as full speed devices support it and is better suited to test the device for critical high speed operation than low speed operation.

3. PROPOSED WORK

Input module: This module converts the serial input of the host. Remember that all data must be packed in packaging that is suitable for the USB protocol. Its implementation uses an 8-bit shift register.

Configuration / Package: This module determines whether the incoming package is a configuration package or a package. This information can be found by recognizing the type and examining the bits of the packet. Of course we can use two comparators to process each packet .

CRC circuit: The USB specification lists two generator polynomials, one for the token and one for the data packet. The generator polynomial for tokens is x 5 + x2 + x0, while the generator polynomial for data packets is x16 + x15 + x2 + x0. Since the remainder is always smaller than the generator polynomial, the CRC token is a bit pattern and the CRC is a 16-bit pattern. Its implementations use XOR gates and D flip-flops.

Address and Register Comparator: If the incoming packet is a configuration, we need to send 0000000 as input to the 7-bit comparator. When a match signal is detected, the address register stores the address. To make this circuit we will need a latch and a comparator.

ACK generator circuit: When a configuration packet is received, we expect an 8-byte data packet to be received and then have to respond with an ACK. The 8-byte data packet contains the newly assigned address.

Packet Data Generator: If the input packet was successfully received by the host, the controller should send the data requested by the host. As mentioned above, this data must be bundled into a packet and then sent serially to the host. We'll use a multiplexer and an 8-bit register to make this circuit.

4. METHODOLOGY USED

ASIC technology is used to design high volume USB 2.0 devices using built-in USB 2.0 support. The operating frequency is low enough to allow data recovery for USB devices at full speed. Can be managed in VHDL providers, encode with ASIC providers. ASIC provider who only provides a simple level translator to meet USB signaling requirements. Door arrangements work conveniently today. The gate arrays operate between 30 and 60 MHz. The existing design method must change as USB 2.0 signaling operates at hundreds of MHz. Without modification, it is difficult to compile VHDL code to increase the operating frequencies. The development of USB 2.0 peripherals is formal for the purpose of UTMI. Peripherals and ASIC development is used to define documents and interfaces.

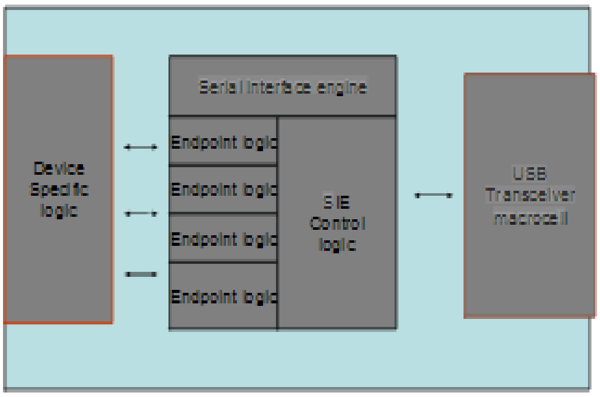


Figure 1: USB 2.0 transceiver

The sender performs various tasks. The conversion of data from parallel to serial is due to the sender. Data generation is one of the functions of the sender. It approves the packets before they are sent to the host. Another function of the sender is to calculate the 16-bit CRC contained in data packets sent to the host. High-level functionality that must be present in the macro cell.

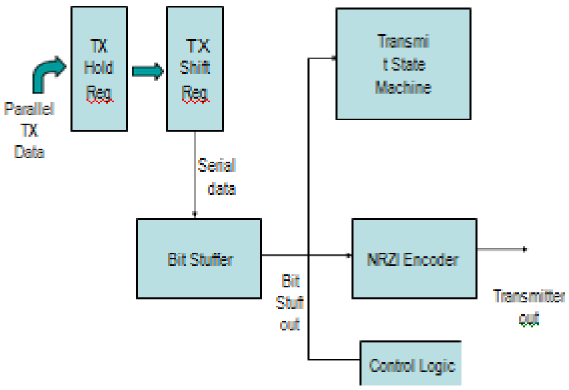


Figure 2: Sender

The function of the receiver is the opposite of the function of the sender. The function of the transmitter is more complicated than that of the transmitter; Both 5-bit CRC and 16-bit CRC are receiver functions. Token packets contain 5-bit CRCs and data packets contain 16-bit CRCs. Therefore 5 and 16 bit CRCs are required. The value is calculated with the information received from the packet are compared by the transmitter. In the event of an inconsistency, a new transmission is requested.

5. RESULT AND DISCUSSION

The USB host controller adequately supports the configuration process by which the device is assigned an address. It then monitors to him addressed bus packets - even - and manages the data transfer to the host computer. The data should be grouped in packets and transmitted to the host. During this time, the validity of incoming packets should be checked using 5 and 16 bit CRCs and 1's complement check bits. The controller can process two types of transactions, which means that it must respond with two packets . The first package is a configuration package. When a SETUP packet is received, it is expected that it receives an 8-byte data packet and that the chip must respond with a signal to acknowledge receipt (ACK) . The 8-byte data packet contains the newly assigned address. We call it the setup process. The second package is an IN package. When an IN packet is received from the host, the controller checks whether the address matches the address assigned to the chip. When a match is found, we send a data packet. We call it the application process. The design process for this chip uses the Finite State Machine (FSM) method, which is based on a modular top-down design approach. Its VHDL code is described at the behavioral or structural level. We then simulate and verify each module we design. The final step is to synthesize your logic circuit and implement your hardware.

5. CONCLUSIONS

The redesigned micro cell of the USB trans-receiver is useful in the hardware architecture of the Linux and Android operating systems for high-speed data communication for the redesigned USB 2.0 device. It has been established that control transfer and isochronous transfer are detected . Control transfer as needed for a new device setup and isochronous as full speed devices support it and is better suited to test the device for critical high speed operation than low speed operation.

REFERENCES

1. Jolfaei F., Mohammadizadeh N., Sadri M., and FaniSani, F. (2009, December). High speed USB 2.0 interface for FPGA based embedded systems. In Embedded and Multimedia Computing, 2009. EM- Com 2009. 4th International Conference on (pp. 1-6). IEEE.
2. Guo G., Li Z., and Yang F. (2011, July). Design of high speed pulse data acquisition system based on FPGA and USB. In Multimedia Technology (ICMT), 2011 International Conference on (pp. 5374-5376). IEEE.
3. Babulu K. and Rajan K. (2008, July). FPGA Implementation of USB Transceiver macro cell Interface with USB2 0 Specifications. In Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on (pp. 966-970). IEEE.
4. Szecowka P. and Pyrzynski K. (2012, September), USB receiver/transmitter for FPGA implementation. In signals and Electronic system (ICSES), 2012 International Conference on (pp.1-6). IEEE.

Lun C., bin Marzuki A. and Wei S. (2012, June). Analog front-end design implementation of USB 2.0 OTG Attach Detection Protocol. In Intelligent and Advanced Systems (ICIAS), 2012 4th International Conference on (Vol. 2, pp. 774-779). IEEE.

ENERGY SAVINGS IN IDLING CONDITIONS OF LOW POWER ASYNCHRONOUS GASP CIRCUITS USING POWER GATING DRIVER STAGE

C.Shanthi[1]., R D Gopal[2]., Mr. B. Naresh Kumar[3]

1 Associate Professor, Department of ECE., Malla Reddy Institute of Engineering & Technology., Maisammaguda., Medchal., TS, India (✉: shanthi @gmail.com)

2 Assistant Professor, Department of ECE., J.B.R.E.C., Yenkapally village., Maisammaguda.,

3 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda.,

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— There are several methods that can be used to reduce the power consumption of digital circuits. One of them is power control. In this project, we are using the grid state maintenance technique to reduce the power consumption of the GasP family of asynchronous digital circuits. The large power consumption in digital circuits is due to leakage currents such as lines below the threshold, junction leaks, and tunnel leaks through the gate oxide. Based on the result of the experiment, it was found that power control is the most effective method to reduce leaks below the threshold. In the power there is a PMOS, an NMOS transistor is used to provide virtual power to the block, which is known as Virtual VDD and Virtual GND. NMOS and PMOS transistors are called sleep transistors. The power control logic activates the device in anticipation of the receive signal

Keywords— GasP, Power Gating, Asynchronous, Lazy Latch, Static Power, Fine Grain Power Gating, Conventional Latch, Power GasP.

1. INTRODUCTION

As with streaming, the use of different process technologies reduces the size of electronic devices, greatly improving chip performance and increasing density, allowing more and more calculations in small areas. Because of the technology, energy consumption is increasing dramatically on a large scale. Nowadays, one day of battery life is cited as a requirement for everyday electronic devices such as cell phones and laptops. Also in servers and advanced computers. A higher energy consumption leads to a heating that requires expensive cooling techniques.

In order to expand the technology, the voltage of the power supply must be reduced in order to avoid destruction of the transistors due to the high electric field. Scaling the supply voltage also saves a significant amount of dynamic energy, but at the expense of performance. In order to maintain the threshold power, the voltage must be scaled. The threshold voltage and the leakage have an exponential relationship. Because the leakage power, commonly known as static power, a large part of the total power consumption.

2. EXISTING SYSTEM

We use a level sustaining power activation technique for the GasP family of asynchronous digital circuits to achieve energy savings. The techniques used make it possible to achieve energy savings by reducing leakage in the rest of the circuit below the threshold. Additional transistors are inserted between the source and the circuit. When the circuit is inactive, additional transistors interrupt power to the circuit. Turning off the power supply decreases the power supply to the voltage circuit at various nodes in the circuit. The below threshold leakage in a transistor depends on the voltage across it. Turning off the circuit to reduce power loss is known as power control.

There may be a loss of energy in the pipeline due to the shutdown. A special circuit is used for each stage in order to avoid loss of state. Steps light up in anticipation of incoming data. Power is restored to each stage when the interlocks are active. We cut the power supply on one level as no status data is lost and the power supply is only switched on when necessary.

3. PROPOSED METHODOLOGY

The new fine-grain power control technology was developed to provide energy savings when idling in asynchronous GasP circuits. The drive stage is controlled by GasP circuits. With the fine grain technique we can switch off the inactive part of the pipe. In this technique, a PMOS and an NMOS transistor are used as a suspension transistor. The fine grain feed gate controls the performance of each individual stage of the pipeline. When the pipe is empty, the individual floors are deactivated. With this technique, the power supply is interrupted even when the pipe is full. The power supply for the combined circuit and the locks is switched off.

Each stage of the pipeline is divided into three parts:

1. Power Trigger Block - This block contains hold transistors for switching on and off.

2. Power GasP circuit: This circuit is used to sequence the data through the latches and generate a power control signal.

3. Locks and Combination Circuits - These circuits are used to store data and require power.

The Power-GasP circuit has the necessary logic to generate the suspend signal. This refers to the power control signal in this document. The power control signal controls the holding transistor in the power control block. The power supply offers virtual, Vvdd and Vgnd power supplies. These power supplies are used for the locks and combinatorial circuits at this stage. The Power GasP circuit is powered by a normal power source.

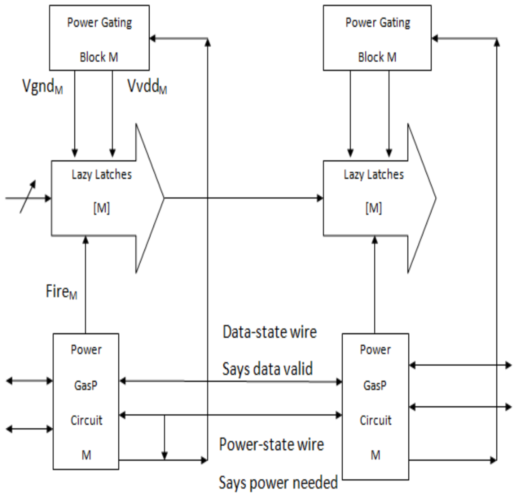


Fig. -1 Function diagram

3.1 Power GasP circuit

The traditional GasP circuit has been modified to include power activation logic and we will call it the Power GasP circuit. The Power Gasp circuit generates a power control signal, a status cable and a fire signal. The power control signal slowly cuts power to the latches, but turns them on quickly to avoid data loss.

Each Power GasP circuit is interlocked and consists of two status wires, a data status wire, and a power status wire.

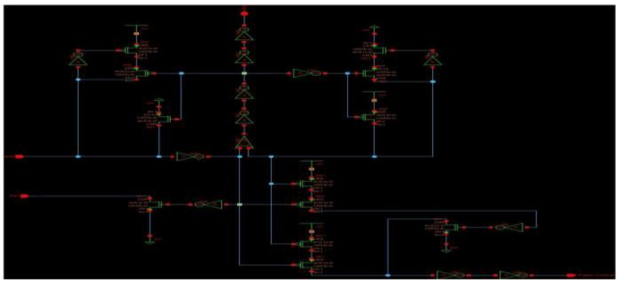


Figure -2: Power GasP

3.2 POWER door unit

The power activation block, which is controlled by the power control signal from the Power-GasP circuit, supplies power to the locks and combinatorial circuits. The power activation block consists of suspension transistors. This power control technique uses two suspension transistors, one is the PMOS transistor, the header, and the other is the NMOS transistor, the footer. The PMOS transistor or header drain acts as a new power supply called the Virtual Vdd or Vvdd. The drain of the NMOS transistor acts as a new ground called Virtual Gnd or Vgnd. The locks and combinatorial circuits are supplied from the new sources Vvdd and Vgnd.

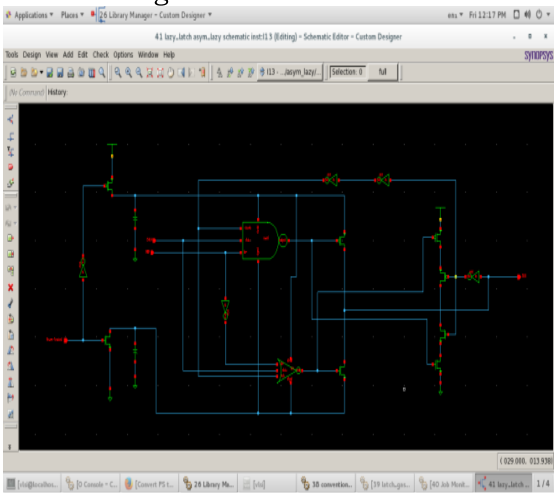

Applications
Places
Library Manager - Custom Designer
Tools Design View Add Edit Check Options Window Help
synopsys

Fig. -3: Rotten bar

3.4 GasP circuits

The GasP family of asynchronous circuits enables control of individual pipes, branching and assembly of pipes, as well as on-demand assembly using arbitration. Two GasP modules that are connected by a single W cable and are known as status cables. GasP uses the capacitance of the wire to store states instead of the switches and latches used to store states in the traditional way. A GasP module changes when its predecessor level offers new data for the next level. The necessary condition for the change is as follows: the previous step is FULL and the next step is EMPTY. Different conventions are used: HI is FULL and LO is EMPTY.

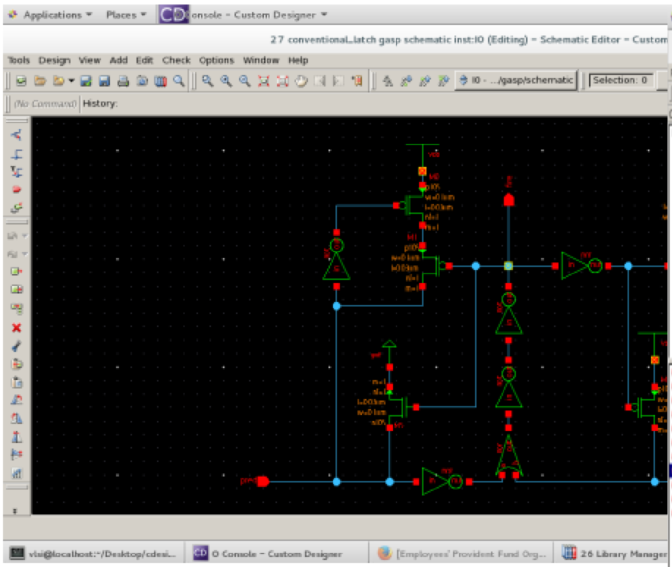
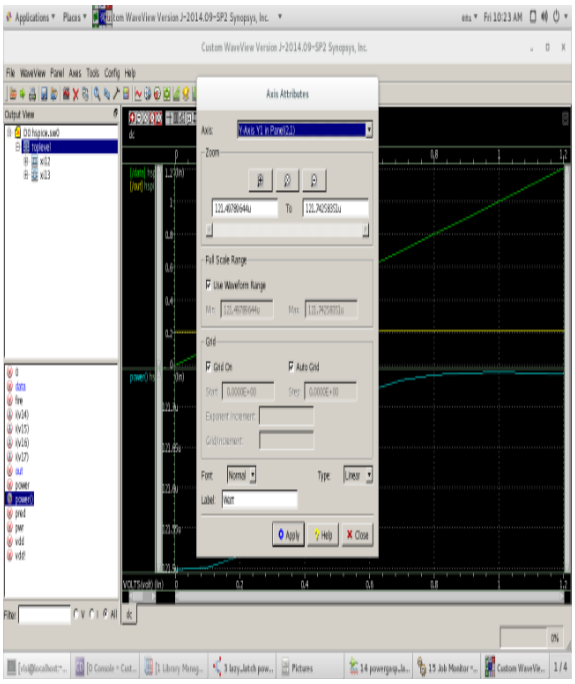

Applications Places Console - Custom Designer
27 conventional_latch gasp schematic inst:I0 (Editing) - Schematic Editor - Custom
Tools Design View Add Edit Check Options Window Help
Selection: 0
History:
vlsi@localhost:~/Desktop/cdesi...
Console - Custom Designer
26 Library Manager

Fig. -4: GasP circuit

4. RESULTS AND DISCUSSIONS

When comparing the results of the conventional lock with GasP circuit with the delayed lock with GasP power supply using current blocking, I found that the total power consumption in the GasP power supply was 3.9 n watts and for the conventional lock with GasP circuit 147 .5 n watts.



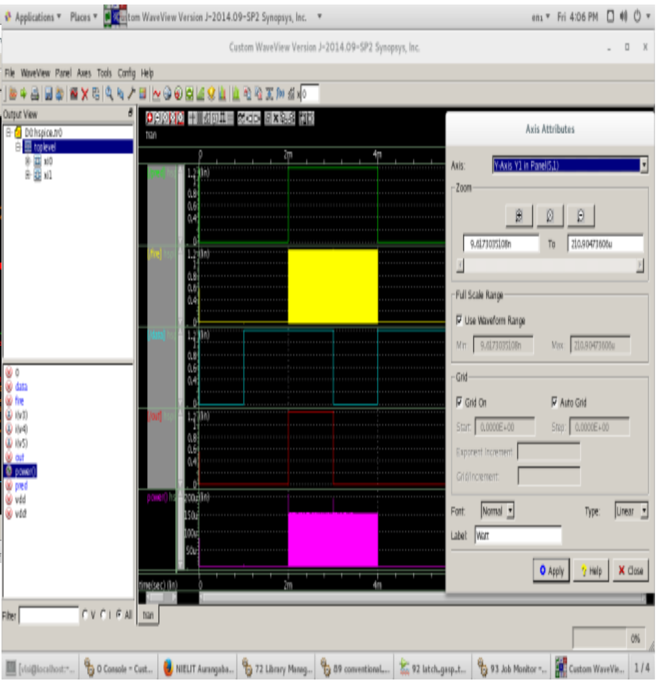
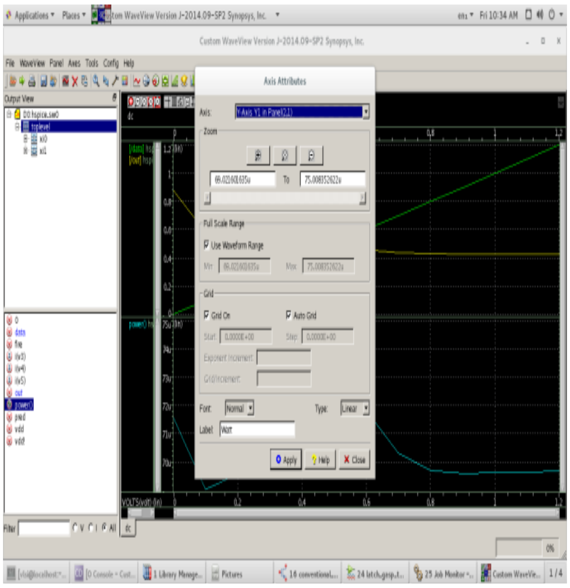
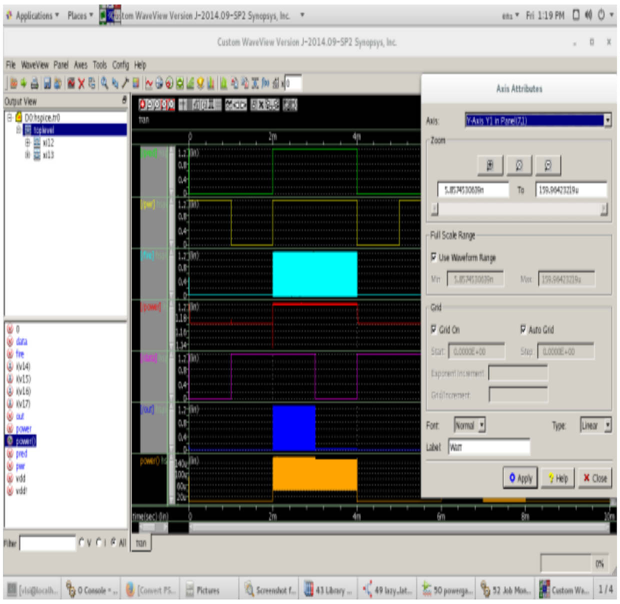


Fig. -5: Conv output waveform. lock with GasP





Axis: Y-Axis Y1 in Panel(7,1)
Zoom: 5.857453063‍9n To 159.96423219u
☑ Use Waveform Range
Min: 5.857453063‍9n Max: 159.96423219u
☑ Grid On ☑ Auto Grid
Start: 0.0000E+00 Step: 0.0000E+00
Font: Normal Type: Linear
Label: Watt

Fig. -6: Lazy latching output waveform with GasP energy

Table 1: Comparison of the required performance

S.No.		Lazy latch with power GasP	Conventional latch with GasP
1.	DC power	69u watt	121.4u watt
2.	Total power	5.8n Watt	9.6n watt

5 CONCLUSIONS

This article uses a fine-grain power control technique for the GasP family of asynchronous circuits. The fine grain feed gate can control the output for each stage of the pipeline. The sleep transistors of each stage control the performance of this stage and its combinational circuit. The stage power supply is switched on before data is received. The power supply is cut off when the board is inactive, either because it is empty or because the pipe is blocked. The control circuit for implementing the power control is simple.

The feed gate is designed for the lazy latch. This document compares an electric hose made of lazy bars with an electric gate and a conventional hose made of conventional bars without an electric gate. The reduced load offered by the lazy latch and the deactivation of the amplifier transistors when they are not needed allow an energy saving of 39.5% during the active period. If no work is done for a long time, energy is saved. The energy savings achieved during the period of inactivity depend on the length of inactivity. The longer the period of inactivity, the greater the energy savings achieved.

REFERENCES

1. Swetha Mettala Gilla, Marly Roncken, and Ivan Sutherland, "Long-Range GasP with Charge Relaxation" IEEE Symposium on Asynchronous Circuits and Systems, 2010.
2. Akhila Abba, " Improved Power Gating Technique for Leakage Power Reduction," International Journal Of Engineering And Science,2014.
3. J. Ebergen, "Squaring the FIFO in Gasp," Proc. of the Seventh International Symposium on Advanced Research in Asynchronous Circuits and Systems, 2001.
4. K.-K. Shyu, C.-Y. Ho, and C.-Y. Chang, "A study on using microcontroller to design active noise control systems," in Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS), Nov. 2014, pp. 443–446.
5. Hong-Son Vu and Kuan-Hung Chen, "A Low-Power Broad-Bandwidth Noise Cancellation VLSI Circuit Design for In-Ear Headphones.", IEEE Trans. Very Large Scale Integration (VLSI) Systems, vol. 24, no. 6, pp. 2013-2025, June 2016.
6. Udit Narula, Rajan Tripathi and Garima Wakhle,"High Speed 16-bit Digital Vedic Multiplier using FPGA " in 2nd International Conference on Computing for Sustainable Global Development ,2015,pp. 121-124.
7. Douglas S.C, Introduction to Adaptive Filters, Digital Signal Processing Handbook., CRC Press LLC, 1999.

MAINTAINING VOICE QUALITY OF INTERCONNECTED CDMA NETWORKS IN CELLULAR COMMUNICATION VIA SATELLITE LINK

K. Narmada[1]., A.Triveni[2]., T. A.Meena[3]., S. A Neha[4]., A.Vardhini[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: narmadakari@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0402, 15RG1A0403, 15RG1A0404, 15RG1A0405), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The CDMA based remote communication system is selected over a satellite link to connect the base station transceiver (BTS) and the base station controller (BSC). This is important in order to overcome communication problems, in particular for natural disasters such as floods, cyclones and tsunamis, etc . Meanwhile, the BTS is most vulnerable to damage when the BTS-BSC connection is broken. In this case, a quick re-establishment of the BTS and BSC connection is required for voice communication between disaster management / emergency response teams etc., with the satellite connection being the only way to solve these problems. The size of the BTS can be a micro with a limited coverage area connected to a portable satellite terminal such as the GSAT-12 terminal for instant communication re-establishment.

Keywords— CDMA, cellular network, BTS, BSC, Matrix eternity, Matrix SETU VGFX, 8 Port D-link, IDIR.

1. INTRODUCTION

We think about the problem of routing packets across a multi-hop network composed of multiple causes of traffic and wireless links while making certain bounded expected delay. Each packet transmission could be overheard with a random subset of receiver nodes among that the next relay is chosen opportunistically. When multiple streams of packets will be to traverse the network, however, it may be desirable to route some packets along longer or even pricier pathways, if these pathways eventually result in links which are less congested [1]. More precisely, the opportunistic routing decisions come in a web-based manner by selecting the following relay in line with the actual transmission outcomes in addition to a rank ordering of neighboring nodes. To make sure throughput optimality, backpressure-based algorithms make a move completely different. This very property of ignoring the price towards the destination, however, becomes the bane of the approach, resulting in poor delay performance in low to moderate traffic. E-DIVBAR is suggested: when selecting the following relay one of the groups of potential forwarders, E-DIVBAR views the sum differential backlog and also the expected hop-count towards the destination. The primary contribution of the paper is to supply a distributed opportunistic routing policy with congestion diversity (D-ORCD) to which, rather of the simple addition utilized in E-DIVBAR, the congestion details are integrated using the distributed shortest path computations. We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed QualNet simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality. Within this work, however, we've selected to concentrate our comparative analysis around the following solutions in literature that have similar overhead, complexity, and practical structure: ExOR, DIVBAR, and E-DIVBAR. Under this insurance policy packets are routed based on a rank ordering from the nodes with different congestion measure [2]. In addition, we suggested an operating distributed and asynchronous 802.11 compatible implementation of D-ORCD, whose performance was investigated using a detailed group of QualNet simulations for practical and realistic systems. The primary challenge in the style of minimum-delay routing policies is balancing the trade-off between routing the packets across the shortest pathways towards the destination and disbursing the traffic based on the maximum backpressure. Compared, D-ORCD may very well be a packet-based form of the min-backlogged-path routing without an excuse for the enumeration of pathways over the network and/or pricey computations of total backlog along pathways. In addition, this paper proposes an operating implementation of D-ORCD which empirically optimizes critical formula parameters as well as their effects on delay in addition to protocol overhead. In addition, while LIFO-Backpressure policy guarantees stability with minimal queue-length variations, realistic burst traffic in large multi-hop wireless systems may lead to queue-length variations and unnecessarily high delay.

2. CLASSICAL DESIGN:

The opportunistic routing schemes could possibly cause severe congestion and unbounded delay. In comparison, you are able to that the opportunistic variant of backpressure, diversity backpressure routing ensures bounded expected total backlog for those stabilizable arrival rates. To make sure throughput optimality, backpressure-based algorithms make a move completely different: instead of using any metric of closeness towards the destination, they pick the receiver using the largest positive differential backlog [3]. Disadvantages of existing system: Other existing provably throughput optimal routing policies distribute the traffic in your area inside a manner much like DIVBAR and therefore, lead to large delay. E-DIVBAR doesn't always create a better delay performance than DIVBAR.

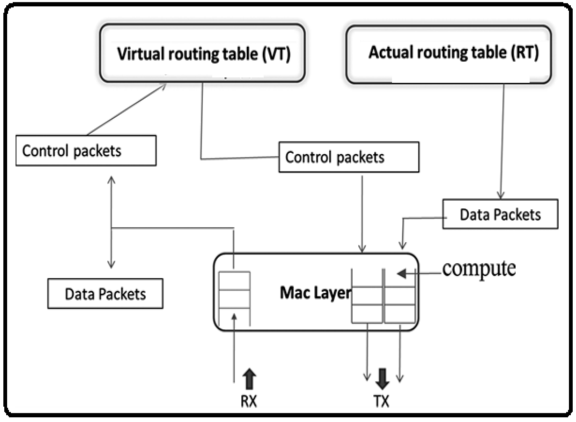


Fig.1.Proposed block diagram

3. ROBUST SCHEME:

An extensive analysis from the performance of D-ORCD is supplied in 2 directions: We offer detailed simulation study of delay performance of D-ORCD. We tackle a few of the system-level issues noticed in realistic settings via detailed simulations. Additionally towards the simulation studies, we prove that D-ORCD is throughput optimal when there's just one destination (single commodity) and also the network are operating in stationary regime. While characterizing delay performance is frequently not analytically tractable, many variants of backpressure formula are recognized to achieve throughput optimality [4]. Throughout the transmission stage, a node transmits a packet. Within this paper, we provided a distributed opportunistic routing policy with congestion diversity by mixing the key facets of shortest path routing with individuals of backpressure routing. Simulations demonstrated that D-ORCD consistently outperforms existing routing algorithms. Benefits of suggested system: We reveal that D-ORCD exhibits better delay performance than condition-of-the-art routing policies concentrating on the same complexity, namely, ExOR, DIVBAR, and E-DIVBAR. We reveal that the relative performance improvement over existing solutions, generally, depends upon the network topology but is frequently significant used, where perfectly symmetric network deployment and traffic the weather is uncommon. The optimality from the centralized option would be established using a type of Lyapunov functions suggested. ***Implementation:*** Throughout the acknowledgment stage, each node which has effectively received the transmitted packet, transmits an acknowledgment towards the transmitter node. D-ORCD then takes routing decisions with different congestion-aware distance vector metric, known as the congestion measure. D-ORCD uses routing table each and every node to look for the next best hop. The routing table at node includes a listing of neighbors along with a structure composed of believed congestion measure for those neighbors in connected with various destinations. The routing table functions like a storage and decision component in the routing layer. The temporary congestion measures are computed inside a fashion much like a distributed stochastic routing computation of utilizing the backlog information at the outset of the computation cycle. More precisely, node periodically computes its very own congestion measure and subsequently advertises it to the neighbors using control packets at times of seconds. More particularly, throughout the relaying stage, the relaying responsibility from the packet is now use a node using the least congestion measure among those that have obtained the packet. The congestion way of measuring a node connected having a given destination provides approximately the perfect draining duration of a packet coming at this node until it reaches destination. Finally the particular routing table is updated while using records within the virtual routing table after every second [5]. Noting the expected transmission time at node for that packet may then be approximated. We discuss the implementation problems with D-ORCD, especially, distributed and asynchronous iterative Computations. We offer a short discussion from the fundamental challenges of D-ORCD such as the three-way handshake procedure employed in the MAC layer, link quality estimation, avoidance of loops while routing, and overhead reduction issues. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively. One of the leading challenges within the implementation of the opportunistic routing formula, generally, and D-ORCD particularly, is the style of an 802.11 compatible acknowledgement mechanism in the MAC layer. Here we propose an operating and straightforward method to implement acknowledgement architecture. Specifically, before any transmission, transmitter performs funnel sensing and starts transmission following the back off counter is decremented to zero. The priority ordering determines the virtual time slot where the candidate nodes transmit their acknowledgement [6]. Nodes within the set which have effectively received the packet then transmit acknowledgement packets sequentially within the order based on the transmitter node. Within our implementation, we've cheated the priority-based queuing D-ORCD prioritizes the control packets by assigning them the greatest strict priority, lowering the probability the packets are delivered to the MAC layer as well as making certain a prompt receiving the control packets. Furthermore, D-ORCD scheduler assigns a sufficiently lower PHY rate for that control packets. In passive probing, the overhearing capacity from the wireless medium is required. The nodes are configured to promiscuous mode, hence enabling these to hear the packets from neighbors. In passive probing, the MAC layer monitors the amount of packets caused by the neighbors such as the retransmissions. We've extended the rule to D-ORCD by advertising the routes as unreachable to greater rated nodes. Particularly, you can easily observe that this overhead cost, i.e., the entire quantity of ACKs sent per data packet transmission, increases linearly with how big the group of potential forwarders. Thus, we think about a modification of D-ORCD by means of opportunistically routing with partial diversity [7]. We think about the modifications of D-ORCD with partial diversity and choose the amount of neighbors which acknowledge the reception from the packet. This analysis characterizes the trade-off between performance and also the overhead cost connected with receiver diversity. In Split-horizon with poison reverse, a node advertises routes as unreachable towards the node by which these were learned. Without effort, this process penalizes the routes with loops and removes them in the group of available alternatives. Finally, a weighted average can be used to mix the active and passive estimates to look for the link success odds.

3. CONCLUSION:

The aim of this paper would be to design a routing policy with improved delay performance over existing opportunistic routing policies. We advise a period-different distance vector, which helps the network to route packets via a neighbor using the least believed delivery time. D-ORCD opportunistically routes a packet using three stages of: transmission, acknowledgment, and relaying. We provided theoretical throughput optimality evidence of D-ORCD. In D-ORCD, we don't model the interference in the nodes within the network, but rather leave that issue to some classical MAC operation. Passive probing doesn't introduce any extra overhead cost but could be slow, while active probing rates are set individually from the data rate but introduces pricey overhead. D-ORCD approximates the reply to the fixed point equation using a distributed distance vector approach. The generalization towards the systems with inter-funnel interference appear to follow along with directly, where, the cost of the generalization is proven is the centralization from the routing/scheduling globally over the network or perhaps a constant factor performance lack of the distributed variants. The implementation of D-ORCD, similar to the opportunistic routing plan, involves selecting a relay node one of the candidate group of nodes which have received and acknowledged a packet effectively.

REFERENCES:

[1] AbhijeetBhorkar, Member, IEEE, Mohammad Naghshvar, Member, IEEE, and Tara Javidi, Senior Member, IEEE, “Opportunistic Routing With Congestion Diversity inWireless Ad Hoc Networks”, ieee/acm transactions on networking, vol. 24, no. 2, april 2016.

[2] L. Ying and S. Shakkottai, “On throughput-optimal scheduling with delayed channel state feedback,” presented at the 2008 Information Theory and Applications Workshop, San Diego, CA, USA, Feb. 2008.

[3] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, “A high throughput path metric for multi-hop wireless routing,” in Proc. ACM Mobicom, 2003, pp. 134–146.

[4] P. Gupta and T. Javidi, “Towards throughput and delay optimal routing for wireless ad hoc networks,” in Proc. Asilomar Conf., 2007, pp. 249–254.

[5] S. Sarkar and S. Ray, “Arbitrary throughput versus complexity tradeoffs in wireless networks using graph partitioning,” IEEE Trans. Autom. Contr., vol. 53, no. 10, pp. 2307–2323, Nov. 2008.

[6] E. Leonardi, M. Mellia, M. A. Marsan, and F. Neri, “Optimal scheduling and routing for maximum network throughput,” IEEE/ACM Trans. Netw., vol. 15, no. 6, pp. 1541–1554, Dec. 2007.

[7] A. SHAIKH, A. VARMA, L. KALAMPOUKAS, AND R. DUBE, “ROUTING STABILITY IN CONGESTED NETWORKS: EXPERIMENTATION AND ANALYSIS,” IN PROC. ACM SIGCOMM,

SEGMENTATION AND CLASSIFICATION OF BRAIN TUMOR FROM MEDICAL IMAGES USING FUZZY-C MEANS AND SVM CLASSIFIER

Manju padidela [1]., A.Priyanka[2]., A.Kavya[3]., A.Pooja[4]., B Aswini[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: cheers2manju@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0406, 15RG1A0407, 15RG1A0408, 15RG1A0409), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— Magnetic resonance imaging is the most important technique in detecting brain tumors. In this document, data mining methods are used to classify magnetic resonance images. A new hybrid technology based on the Support Vector Machine (SVM) and diffuse c-means is proposed for the classification of brain tumors. The proposed algorithm is a combination of Support Vector Machine (SVM) and Fuzzy-C means, a hybrid technology for predicting brain tumors. This algorithm enhances the image using enhancement techniques such as contrast enhancement and stretching in the middle area. Double threshold and morphological operations are used to remove the skull. Diffuse c-means clustering (FCM) is used for image segmentation to identify the suspicious area on the brain's MRI image. The grayscale line length matrix (GLRLM) is used to extract features from the brain image. Then the SVM technique is applied to classify the MRI images of the brain and provide precise and most accurate MRI images to the brain.

***Keywords*— Brain tumour, clustering, GLRLM, SVM**

1. INTRODUCTION

Data mining can be a simple and robust tool for extracting data from a massive data set [1]. Classification is a branch of data mining. Many classification techniques for medical imaging are available in this area, such as the artificial neural network (ANN), the fuzzy mean (FCM), the support vector machine (SVM), the decision tree and the Bayesian classification. Different researchers classification techniques for classification of medical images implemented. Segmentation is a technique for extracting suspicious areas from images. In this article, the segmentation technique was carried out using FCM aggregation (Fuzzy C-Mean) [2]. The skull was masked prior to using the FCM agglomeration technique. Extracting functions means that you are supplying information from the image. The strategy uses the grayscale run length matrix (GLRLM) to extract the function [3]. Reduced GLRLM scores are described to aid the vector machine in training and testing. MRI images of the brain have been differentiated using SVM techniques, which are widely used to analyze information and recognize patterns. Create a hyperplane between the information sets to indicate the category to which it belongs [4]. The main goal of this work is the development of a hybrid technique with which images by magnetic resonance of the brain can be classified successfully and efficiently with Fuzzy C - including this and the vector machine of support (SVM).

2. RELATED WORK

Support vector machines have been used in many studies in [4-6]. HB Nandpuru, Dr. SS Salankar and educational. VR Bora worked on the classification of brain cancer by magnetic resonance imaging using a carrier vector machine. Support vector machines (SVMs) were used to classify brain imaging. This article discussed feature extraction from MRI images of the brain using grayscale, symmetry, and texture features. They achieved an intelligent result [4]. A. Padma and R. Sukanesh their study of SVM based on the classification of enjoyment tissues in the CT image of the brain by using the wave-based dominant grayscale dash lengths texture function . They highlighted the technique of medical CT imaging as one of the widely and reliably applied techniques for detecting and efficiently localizing pathological changes using SVM. They achieved an accuracy of 98% [5] . SHSA Ubaidillah, R. Sallehuddin, and NA Ali, who work in cancer, discovered the use of artificial neural networks and assistive vector machines: a comparative study. In this article, they adjusted the performance of four completely different cancer records using the SVM and ANN classifiersSVM with a performance sensitive to records with fewer input characteristics (breast cancer and gonads). Liver cancer), but ultimately the SVM classifier gave a higher result for growth [6].

3. PROPOSED METHODOLOGY

The recommended method includes a collection of phases of clustering of magnetic resonance images in the brain. The main steps are shown in Figure 1. This hybrid technique includes the following major steps such as enhancement, cranial banding, segmentation, feature extraction, and SVM classifier training using GLRLM magnetic resonance imaging, information recording and review. All surface units of the above steps are classified in the test part Classification of new MRI images with GLRLM function for SVM and MRT imaging of the brain. This study used an MRI dataset to image the brains of 120 patients and classified them as simple and abnormal. The image is processed by:

- Image Reading
- MRI images Enhancement
- Striping of Skull step
- Segmentation using Fuzzy c-means
- Feature Extraction
- Support Vector Machine Classifier

3.1 Playback of pictures

MRI images of the brain were collected from various medical centers. These brain MRI images were converted into 2D arrays.

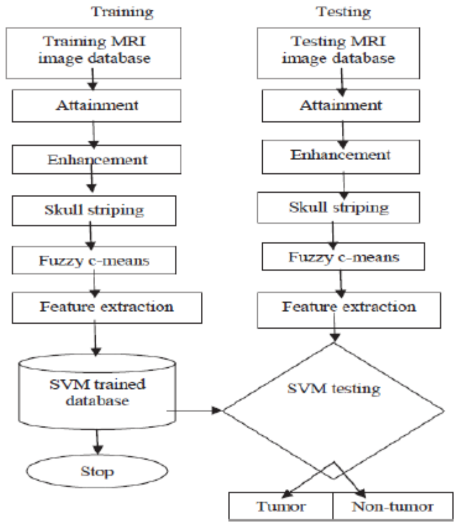


Fig. 1: Proposed classification system.

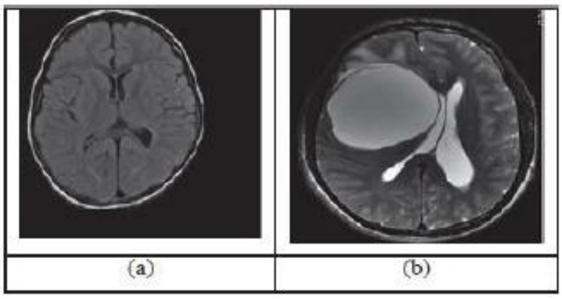


Fig. 2: (a) Non-tumor MRI image (b) Tumor MRI image

3.2 Improvement of magnetic resonance images

The image quality is improved by an enhancement method. It is important to improve the image information for the human viewer in order to get the correct results. The remedies listed below are used to improve the brain's MRI image. The first step is to improve the MRI. Here only the brightness of the photos was increased in order to improve the perceptibility. This was done to improve the quality level of the brain's MRI images. Contrast enhancement: MRI images are RGB images that are converted to grayscale images. Then, by applying the above function f (xij), the grayscale images are converted to indexed images. The output images obtained after applying the whole process are used to improve the quality of the images.

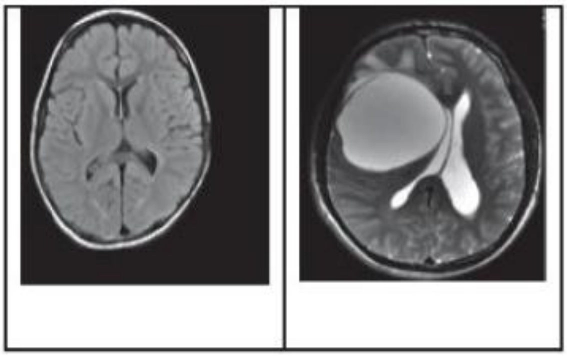


Fig. 3: (a) Improved non-tumor image (b) Improved tumor image

3.3 Skull extraction step

Removing the skull is a remarkable step. The steps to remove the skull are given below.

• Double Threshold: This is a segmentation technique. This method converts the image in binary form, that is, a grayscale image, into a binary image. This method creates the mask by setting each pixel in the range [0.1 * 255-0.88 * 255] to 1 (white) and the remaining pixels to zero (black). Pixels from non-brain tissue were discarded on the MRI image. Here, 2000 are considered as the upper and lower, which is why we speak of a double threshold technique [7].

• Erosion - At this level, unwanted pixels are clipped from the MRI image past the threshold. Hence, the areas of the skull are removed. Here a 3-radius disk has been used as a structuring element to remove unwanted pixels that help MRI images of the brain.

• Fill in the areas: This technique is used to countersink the holes in the pictures. After the erosion, the altered images are filled using the area fill algorithm . Here, the associated background pixels are converted into foreground pixels so that the holes in the MRT image of the brain that are present in the eroded images are removed.

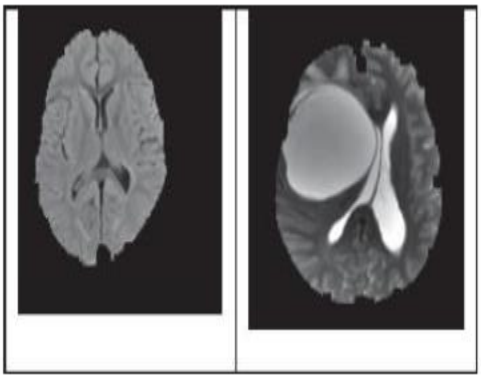


Fig. 4: (a) Masking of the skull non-tumor image (b) Masking of the skull Image of the tumor

3.4 Segmentation with Fuzzy C Means

Segmentation is the method of separating an image into different parts and areas of objects. Images of skull stripes are used in image segmentation. This provides a good result for tumor segmentation. In this work the Fuzzy-C-Means-Algorithm was used to segment magnetic resonance images. The Fuzzy C-Means (FCM) algorithm is used to identify the suspicious area from the MRI image of the brain. This fuzzy method for grouping c-means gives a good segmentation result.

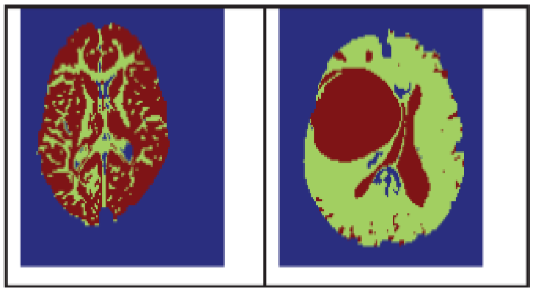


Fig. 5: Fuzzy Mean C algorithm

3.5 Extraction of Features

Feature extraction is a method of finding related features in the image so that the image can be easily understood. This image of the input data group is converted into a compressed form and referred to as feature extraction. You can reduce post-processing work, such as B. the classification of images. The GLRLM feature extraction method is used here. GLRLM is used according to the fuzzy C mean value algorithm.

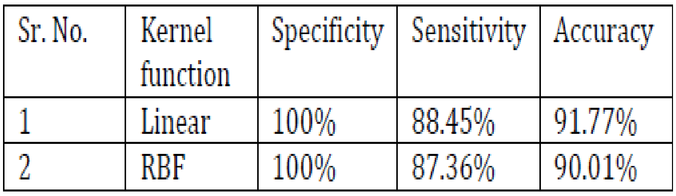
3.6 Support Vector Machine Classifier

SVM is a supervised learning technique. It's a better tool for data analysis and classification. The SVM classifier can be learned quickly, even with large amounts of data. SVM is used for classification questions of two or more classes. Support Vector Machine depends on the design of the decision plans.

4. RESULTS ANALYSIS

This article uses the diffuse c-mean SVM technique to segment and classify MRI images of the brain. An actual data set of 124 MRI brain images were used to acquire "tumor" and "non-tumor" MRI images. Soft tissues in brain MRI imaging are segmented using a double threshold, morphological features and a fuzzy C-mean algorithm for clustering and a grayscale line length matrix for feature extraction. The SVM classifier is trained using 100 brain MRI images, after which the remaining 24 brain MRI images were used to test the trained SVM. The classification result offers precision for large amounts of data.

Table 1: Results of the SVM classification



Sr. No.	Kernel function	Specificity	Sensitivity	Accuracy
1	Linear	100%	88.45%	91.77%
2	RBF	100%	87.36%	90.01%

5. CONCLUSIONS

In this proposed system, brain MRI techniques have proven to be an important means of detecting brain tumors. The hybrid method of collecting support vector machines and fuzzy grouping c-means for classification provides an accurate result for identifying the brain tumor. A hybrid SVM algorithm is proposed for future work in order to obtain a better accuracy rate and a lower error rate. In future work, various data mining techniques can be used to train with various kernel functions to improve classifier performance, and datasets can also be increased.

REFERENCES

1. A.Padma and R. Sukanesh, “SVM based classification of soft tissues in brain CT images using wavelet based dominant gray level run length texture features”, middle-east journal of scientific research, 2013, 13(7): 883-888.
2. S.H.S.A. Ubaidillah, R. Sallehuddinand N.A. Ali, “Cancer detection using artificial neural network and support vector machine: A Comparative study”, jurnal teknologi (science & engineering), 2013, 65:1.
3. O.P. Verma, M. Hammandlu, S. Susan, M. Kulkami and P.K. Jain, "A simple single seeded region growing algorithm for color image segmentation using

adaptive thresholding," 2011 International Conference on Communication Systems and Network Technologies, ©2011 IEEE.

4. Prakash Mahindrakar and Dr. M.Hanumanthappa, “Data Mining In Healthcare: A Survey of Techniques and Algorithms with Its Limitationsand Challenges”, Int. Journal of Engineering Research and Applications,ISSN : 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013, pp.937-941.
5. Kailash Sinha, G.R.Sinha, “Efficient Segmentation Methods for Tumor Detection in MRI Images”, 2014 IEEE Student’s Conference on Electrical, Electronics and Computer Science, 978-1-4799-2526- 1/14/$31.00 ©2014 IEEE.
6. R. S. Raj Kumar and G. Niranjana, “Image Segmentation and Classification of MRI Brain Tumor Based on Cellular Automata and Neural Networks”, IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.
7. H. B. Nandpuru, Dr. S. S. Salankar, Prof. V. R. Bora, MRI brain cancer classification using support vector machine. 2014 IEEE Students 'Conference on Electrical, Electronics and Computer Science, 978-1- 4799-2526-1/14/$31.00 ©2014 IEEE

DESIGN AND IMPLEMENTATION OF D-FLIP-FLOP, AND JK-FLIP-FLOP USING DUAL-MODE LOGIC WITH POWER-UP PROCEDURES

Chintala keerthi [1]., B.Lohitha[2]., B.Madhuri[3]., B.Lahari[4]., B.Bavitha[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: keerthureddychinthala@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0410, 15RG1A0411, 15RG1A0412, 15RG1A0413), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— In this article, we outline the design and implementation of D-FLIP-FLOP, and JK-FLIP-FLOP using dual-mode logic with power-up procedures. This model is used to design successive circuits with the circuit made in TANNER, the output waveform displayed in W-EDIT, and the delay calculated. For these circuits, average power calculations have been made for the value of the d power supply, i.e. 1.2V, TSMC0 is used.

Keywords— D- FLIP-FLOP, J-K FLIP-FLOP, TANNER EDA TOOL

1. INTRODUCTION

LUCIDITY optimization and recital are fundamental tasks for digital circuit designers. The logical effort method (LE) should be proposed in order to easily and quickly evaluate and optimize the delay in logical CMOS paths. As the LE method has become a very popular tool for design and development purposes, it has been adopted as the basis for various computer-aided design tools. DML doors are manufactured at a very high speed. Although LE is primarily used for common CMOS logic gates, it is also useful for other logic families such as pass-through logic. Dual Mode Logic (DML) that converts between two operating modes. It is included in 1) static mode and 2) dynamic mode. Static mode must be stable and have very low performance. The dynamic mode makes the logic mode very fast and not constant. It offers great elasticity. Intimate dual-mode logic cannot use a logical energy policy.

2 PROPOSED SYSTEM

In order to reduce the power in the circuits, two power activation procedures are initiated, namely the suspension technique and the stack suspension technique, and the best technical results are determined.

1. Sleep technique:

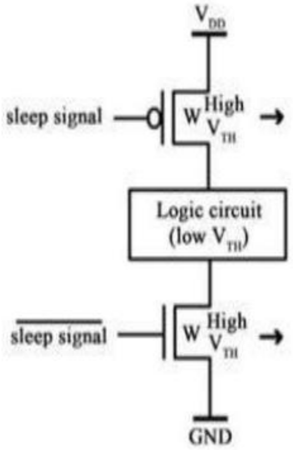


Fig. -1: Sleep technique

In this method, the suspension transistor is used between the VDD and the pull-up network and between GND and the pull-down network.

2. Sleep stacking technology

The mandatory sleep stack and transistor techniques are collective to achieve the sleep stack structure. The role of the sleep transistors in the sleep stack is the same as that of the sleep transistor in the sleep transistor method.

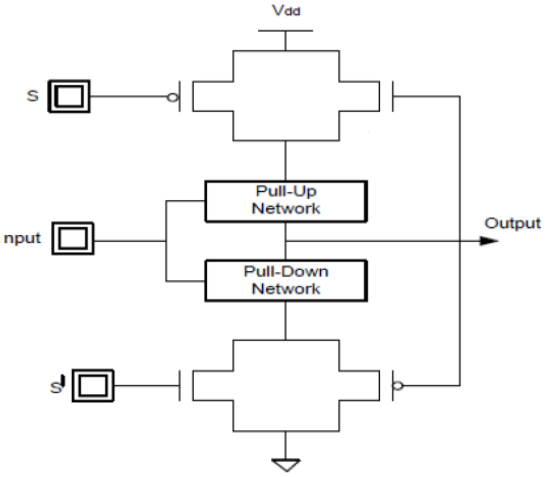


Fig. -2: Sleeping stacking technology

3. Double sleep technique

The double sleep tactic has the advantage that the two additional traction transistors and two additional traction transistors are used in the standby mode, either in the OFF state or in the ON state. In normal mode, when S = 1, the NMOS pull-down transistor is in the ON state and in the pull-up network, the PMOS holding transistor is in the ON state of S ‟= 0. During the state out of the Standby mode is S. is forced to 0 and so the NMOS pulldown transistor is in the OFF state and the PMOS transistor in the ON state and in the pull-up network the PMOS holding transistor is OFF, during the NMOS -Holding transistor is ON.

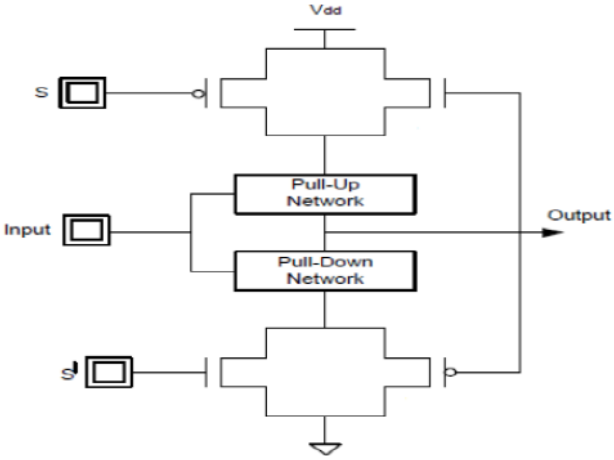


Fig. -3: Double sleep technique

3. RESULT ANALYSIS

Although below the threshold DML gates are effective in dynamic mode, they improve speed over standard CMOS while distributing more power, and in static mode a reduction in performance excess is achieved at the expense of reduced performance. Different power control methods applied to DML logic have more concentrated power dissipation. The LE approach for CMOS-based logical DML networks was introduced.

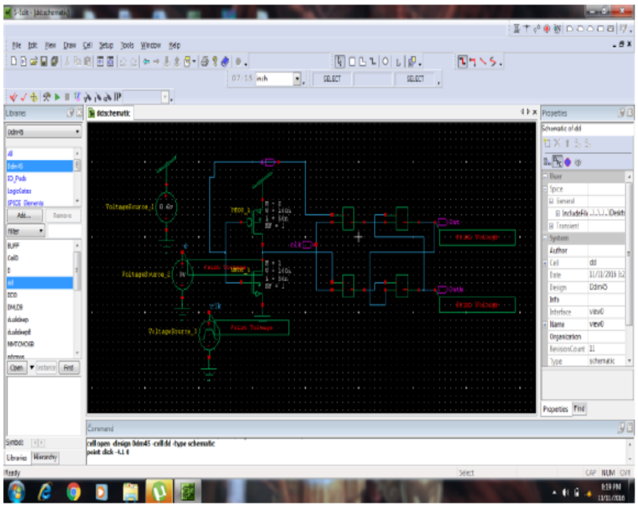


Fig. -4: D flip-flop in the Tanner EDA tool

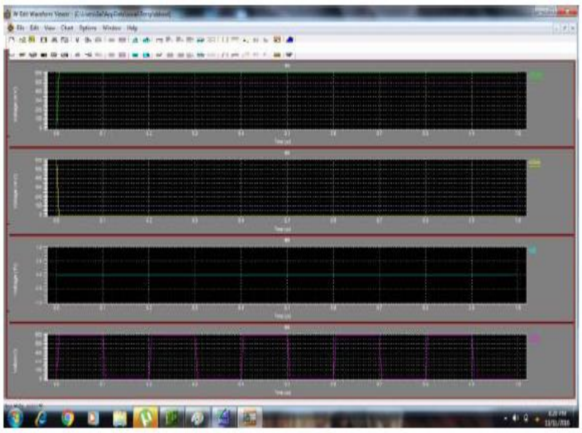


Fig. -5: Flip-flop D waveform in the Tanner EDA tool

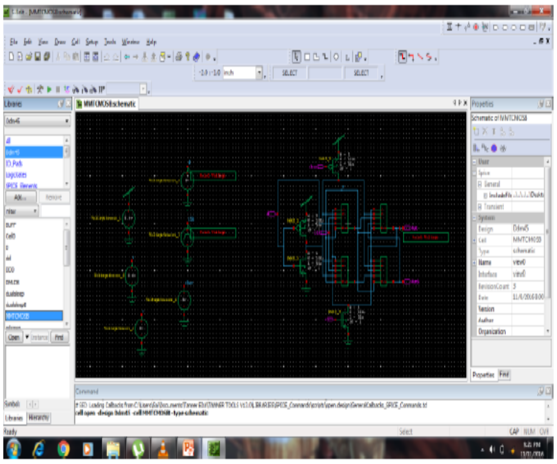


Fig. -6: Switch D in the Tanner EDA tool using the Sleep A technique

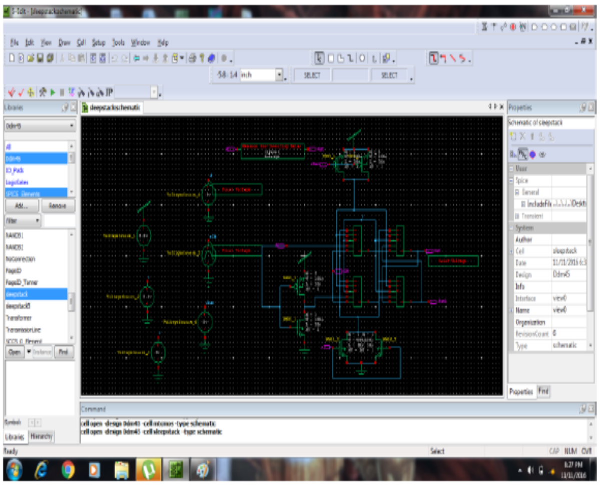


Fig. -7: D flip-flop in the Tanner EDA tool with the stack technology

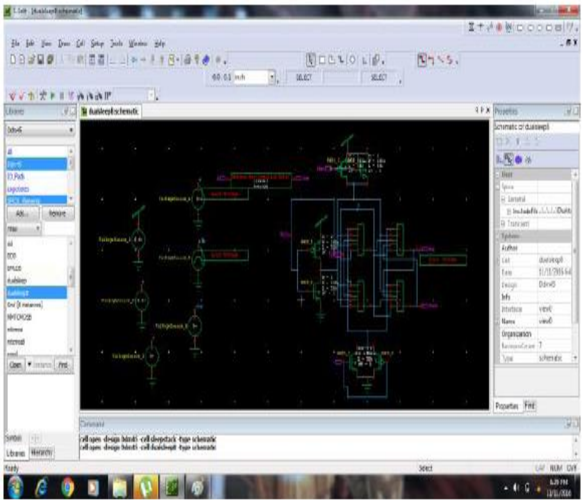


Fig. -8: D flip-flop in the Tanner EDA tool with the double sleep technique

4. JK FLIP-FLOP

The JK rocker is the most practical of the basic rockers. It has the input tracking nature of the synchronized D flip-flop, but has two inputs, usually labeled J and K. If J and K are different, the Q output takes the value J on the next clock edge. The entrances are marked J and K in honor of the aircraft architect Jack Kilby.

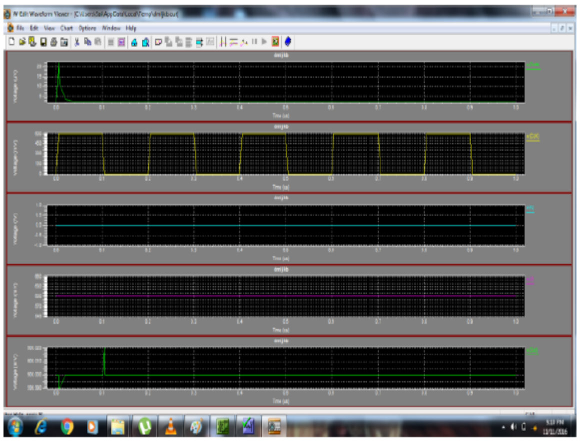


Fig. -9: JK flip-flop waveform in the Tanner EDA tool

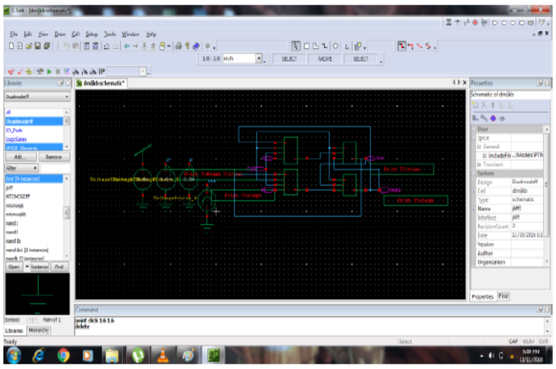


Fig. 10: JK flip-flop in the Tanner EDA tool

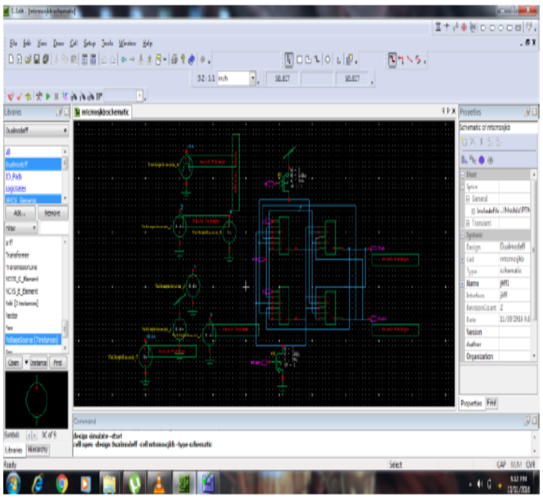


Fig. -11: JK flip-flop in the Tanner EDA tool with sleep technology

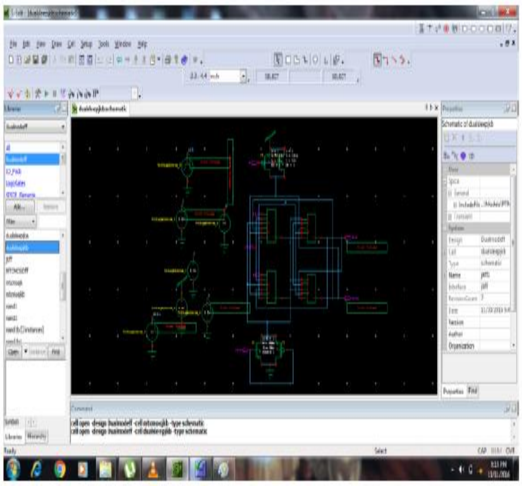


Fig. -12: JK flip-flop in the Tanner EDA tool with sleep stack technology

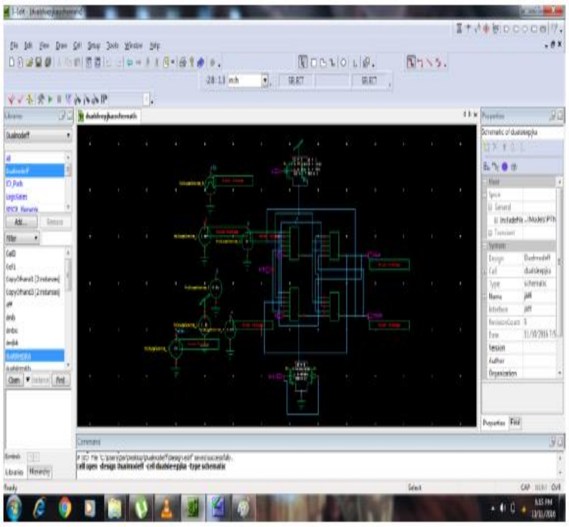


Fig. -13: JK flip-flop on the Tanner EDA tool in the double-stack process

This model is used to design successive circuits with the circuit made in TANNER, the output waveform displayed in W-EDIT, and the delay calculated. For these circuits, average power calculations have been made for the value of the d power supply, i.e. 1.2V, TSMC0 is used.

6. CONCLUSIONS

Although below the threshold DML gates are effective in dynamic mode, they improve speed over standard CMOS while distributing more power, and in static mode a reduction in performance excess is achieved at the expense of reduced performance. Different power control methods applied to DML logic have more concentrated power dissipation. The LE approach for CMOS-based logical DML networks was introduced. The proposed approach allowed for efficient optimization of DML logical networks for a given performance in dynamic operating mode, which was the subject of this article. The DML logic optimized according to the proposed LE methods enabled greater flexibility in the optimization of various DML network structures. This optimization took advantage of the inherent properties of DML for very low dependent capacitance and very low power dissipation in static mode of operation.

REFERENCES

1. Itamar Levi, Ori Bass, Asaf Kaizerman, Alexander Belenky , High Speed Dual Mode Logic Carry Look head Adder , IEEE Trans. Very Large Scale Integration, May 2012.
2. W.M.Pensey and L. Lau, MOS Integrated Circuits. New York: Van No strand, 1972, pp. 260–282.
3. B. Zhai, S. Hanson, D. Blaauw, and D. Sylvester, “Analysis and mitigation of variability in sub threshold design,” in Proc. Int. Symp.Low Power Electron. Design, Aug. 2005, pp. 20–25.
4. Levi, A. Kaizerman, and A. Fish, “Low voltage dual mode logic: Model analysis and parameter extraction,” Excepted Elsevier, Micro electron. J., vol. 12, no. 1, Jan. 2012.
5. Itamar Levi, Alexander Belenky, Alenxader Fish, Logical Effort for CMOS Based Dual Mode Logic Gates , IEEE Transactions On Very Large Scale Integration(vol-22), May 2014.
6. Kaizerman, S. Fisher, and A. Fish, “Sub threshold dual mode logic,” IEEE Trans. Very Large Scale Integration. (VLSI) Syst., vol. 21, no. 5, pp. 979–983, May 2013.
7. M. Alioto, “Ultra low power VLSI circuit design demystified and explained: A tutorial,” IEEE Trans. Circuits Syst. I, vol. 59, no. 1, pp.3–29, Jan. 2012.

A REVIEW ON CHANNEL ESTIMATION ALGORITHMS IN MIMO OFDM BASED WIRELESS SYSTEM FOR DIFFERENT MODULATION SCHEMES

Ch. Keerthi[1]., M.Anjali[2]., M.Shivani[3]., M.sravya reddy[4]., M.Lahari[5]

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: keerthureddychinthala@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0477, 15RG1A0479, 15RG1A0480, 15RG1A0481), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— A modern wireless broadband system from MIMO-OFDM (Orthogonal Frequency Division Multiplexing with multiple inputs and multiple outputs) is more popular due to its good data rate and robustness against multipath fading and high speed. 'Good spectral efficiency. This system offers reliable communication and wide coverage. A major challenge for the MIMO OFDM system is the exact retrieval of channel status information (CSI) and the synchronization between transmitter and receiver. Channel status information is obtained using various estimation algorithms, such as: B. pilot-assisted, blind and semi-blind channel estimation. This article examines the analysis of the channel estimation performance by different algorithms to estimate the channel using different modulation schemes. The channel estimation is based on the least squares and least squares channel estimation algorithms. This article describes the basic introduction of the OFDM system MIMO-OFDM and explains the various channel estimation algorithms.

Keywords— MIMO (Multiple Input Multiple Output), OFDM (Orthogonal Frequency Division Multiplexing) Channel Estimation, CSI, LS Estimation, MMSE Estimation.

1. INTRODUCTION

MIMO is a system with several inputs and outputs. It is used to transmit and receive multiple signals at the same time using multiple antennas on the transmitter and receiver side. Using multiple antennas on the transmitter and receiver side eliminates the problem caused by multipath fading. The system also needs the modulation techniques to send the signal. The OFDM modulation technique is discussed here. The system requires a modulation technique because the communication signal or the voice signal cannot travel long distances due to the low frequency. The modulation technique is a technique in which the change in the characteristics of the carrier signal with respect to instantaneous characteristics such as message / voice signal occurs. The proposed design has improved the representation of the error rate when evaluated with other precoding schemes. In [8], Saeed and Witold considered a multi-user Gaussian transmission channel. They applied the block bias zero forcing precoding technique to get the most optimized channel and showed that this scheme is indeed an optimal multi-user zero forcing precoding under the total of the performance constraint.

2. RELATED WORKS

KG. Wu et al. [1]: In this study, a recursive LS estimator was proposed to improve the performance of DDCE in OFDM systems with transmission diversity. Wu and Chang proposed a regulated LS estimator to improve DDCE performance in OFDM systems with transmission diversity. The proposed method contains the last channel estimate as a priori information in order to alleviate the error propagation problem of the standard LS method. The regularization parameter is derived to fit the MSE of the last estimate and that of the current standard LS estimate. At lower SNR values, when the standard LS method suffers more from the error propagation problem, the proposed method significantly improves the performance of the channel estimation.

MN Seyman et al. [2]: Seyman suggested that the experimental results use particle swarm optimization (PSO) to optimize both the location and performance of the comb-like pilot tones used in the LS channel estimation algorithm in MIMO OFDM systems. . that the optimized pilot tones derived from PSO with respect to MSE and BER performed better than the orthogonal and random pilot tones. In addition, simulations were performed on channels with different values of Doppler changes to show the effect of Doppler changes on the performance of different pilot noises.

Y. (G.) Li et al. [3]: Li suggested that the estimation of channel parameters is an important task in OFDM systems. They presented criteria for the optimal design of training sequences for OFDM systems with multiple transmit antennas and also simplified previously developed channel parameter estimators. With the help of the design criteria, we can create training sequences that not only optimize but also simplify the channel estimation during the training period. The simplified estimator performs similarly to that, but with much less complexity.

J. Ran et al. [4]: Ran proposed the concept of a system and the results of a decision-based channel estimation technique. The improvement in the performance of Decision Directed Channel Estimation (DDCE) compared to the pure preamble-based method is discussed. On the one hand, the DDCE method uses the decisions at the output of the demodulator, which leads to a relatively low complexity and to a single OFDM symbol delay . Overall, the DDCE method shows a good increase in performance with little computing effort.

3. MIMO OFDM PROPOSED SYSTEM

In contrast to conservative FDM, with OFDM a spectral overlap between subcarriers is permitted, since the orthogonality ensures the separation of the subcarriers at the receiver level, offers better spectral efficiency and the use of a steep bandpass filter is not required. The serially transmitted data is sent to the QAM modulator which is used to convert the signal to parallel and the IFFT is used to mix the frequency of different values and guard intervals are inserted to bypass the ISI. DACs are used to convert digital to analog conversion for time division signal transformation. On the receiver side, an analog-to-digital converter and a guard callback are used to remove the guard band.

When using several narrowband channels, the signal is split up and distributed over these channels at different frequencies. This technique reduces the effect of interference that occurs between adjacent channels in the form of frequencies. It transmits the signal over the same period of time, but on different frequencies. Orthogonal frequency division multiplexing (OFDM) with multi-stream antennas can improve the quality and capacity of broadband.

MIMO-OFDM is simple and efficient in managing multiple paths. OFDM is a multi-carrier modulation technique. It contains multiple carriers within the allotted bandwidth to carry data from the source to the destination. Multiple parallel narrowband subcarriers are used instead of a single broadband carrier to carry information. In [11] a MIMO system was proposed which, when used with OFDM, contains less ISI and also leads to less fading and higher data rates. However, as a result of the estimation of noisy channels performed with frequency selective quick change channels, the performance of the MIMO system deteriorates. In [12] he examined the space-time coding delay, the permutation and the multiplicity of the transmitter in combination with the multiplicity of the OFDM two-branch receiver used in high-speed wireless networks.

4. RESULTS OF CHANNEL ESTIMATE

Channel estimation is a critical approach used in wireless cellular network systems where the wireless channel switching occurs in conjunction with a specific point in time generated primarily by a mobile transmitter or receiver at the speed of private cars. Mobile wireless communication is reluctantly affected by obstacles in multiple paths due to reflections and surrounding elements such as mountains, infrastructure, and other obstacles. The system requires an explicit evaluation of the time-varying channel in order to achieve improved and reliable data rates on the receiving side. In particular, the author's motivation was to reduce the problem of desired matrix inversion for each symbol of OFDM data.

The Adaptive Least Squares (ALS) algorithm Recursive Least Squares (RLS) is a robust filter that finds the coefficients recursively, thus helping to reduce a linearly weighted least squares cost function that is consolidated in input signals. The ALS is a reference

Different methods of channel estimation

1. Pilot-assisted channel estimation: The pilot-assisted method develops a known pilot symbol or a known training sequence. This known symbol is used to obtain the channel estimation parameter. These well-known symbols are located between the frame of the transmitted signal and that sent over the channel. On the receiver side, the channel estimation is carried out using the received signal and the known pilot sequence. These pilot-assisted algorithms are used in communication systems because this system has high precision and low computational effort.

In the heterodyne amplification method, the pilot signal is superimposed on the information signal. The entire transmitted frame can be used to transmit the information symbols. This overlay method is more bandwidth efficient than the traditional method. The overlay training method is widely used by research in many research activities.

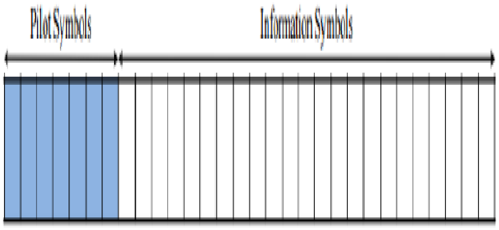


Fig. 1: Classic approach with pilot symbol support

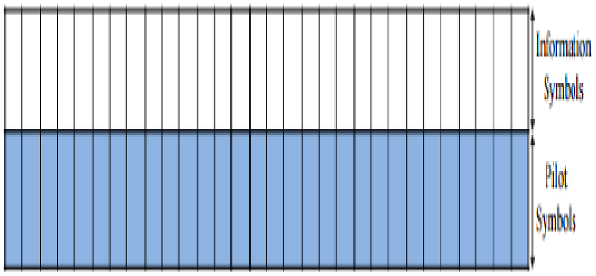


Fig. 2: Layer diagram

2. Blind channel estimation method: With blind channel estimation, no training data is required and the receiver does not know the transmitted sequence. This method requires higher data rates. In order to perform the channel estimation in this method, the statistical properties of the communication signals are essential, but in general the training sequences are used for the channel estimation in static or slowly changing propagation environments.

3. Half-blind channel estimation method: The half-blind scheme is a hybrid method that combines the phenomenon of blind estimation with a limited amount of pilot data. These methods depend on a limited amount of pilot data. The semi-blind method increases the speed of convergence and performs robust tracking of time-varying channels.

4. Decision Channel Estimation Method: Using the previous channel estimate, the data is found and applied to estimate the channel in the last snapshot called the decision direction. With this method, an entire transmission session can be used to transmit data symbols. The statistical properties of the communication channel and the received information symbols are used to estimate the CSI in the channel decision estimation process.

5. OFDM APPLICATION

• Wireless Local Area Network (WLAN) IEEE802.11a / g / n: This is a wireless computer network that connects two or more devices using a wireless method (OFDM) in a limited area such as home, school, or office building. This makes the user mobile but still connected to the network. Most modern WLANs are based on the IEEE 802.11 standard and are sold under the brand name Wi-Fi.

• DAB (Digital Audio Broadcasting): is a digital radio technology for broadcasting radio stations that is used in various countries. It can transmit text, images and audio in a system bandwidth of 1.5 MHz.

• DVB (Digital Video Transmission): is a series of internationally recognized standards for digital television. It is used in DVB-T for terrestrial television systems and in DVB-H for portable devices. Supports HDTV (High Definition Television).

• 3PPG LTE (Long Term Evolution of the third generation partnership project): OFDM is used in 3GPP UMTS (Universal Mobile Telecommunication System) and in 4G LTE in downlink communication. LTE is a 3GPP standard that offers an uplink speed of up to 50 Mbit / s and a downlink speed of up to 100 Mbit / s. LTE will bring technical advantages to the cellular network.

6. CONCLUSION

In this work it is concluded that MIMO OFDM systems have the inherent ability to meet the requirements of future wireless communication systems through the use of channel estimation techniques. The various channel estimation techniques such as learning-based algorithms, blind channel, half-blind channel and their performance are also discussed. The MMSE channel estimator is complex, but faster than the LS and ALS estimators.

REFERENCES

1. B. L. Saux and M. Helard, “Iterative Channel Estimation based on Linear Regression for MIMO-OFDM System,” IEEE international Conference on Networking and Communications, vol.1, no.1, pp. 356-361,2006.
2. Y. Li, J. C. Chuang and N. R. Sollenberger, “Transmit diversity for OFDM systems and its impact on high-rate data wireless networks”, IEEE J. Sel. Areas Communication, vol. 17, pp. 1233–1243,1999.
3. H. Minn, “A reduced complexity channel estimation for OFDM systems with transmit diversity in mobile wireless channels”, IEEE Trans. Commun., vol. 50, no. 5, pp. 799–807,2002.
4. Lyman, J. Raphael, and W. W. Edmonson, “Decision-directed tracking of fading channels using linear prediction of the fading envelope”, In Signals, Systems, and Computers, 1999. Conference Record of the Thirty-Third Asilomar Conference on, vol. 2, pp. 1154-115,1999.
5. Y. (G.) Li, “Simplified Channel Estimation for OFDM Systems with Multiple Transmit Antennas,” IEEE Trans. Wireless Comm., vol. 1, pp. 67–75, Jan. 2002.
6. J. Ran, “Decision-Directed Channel Estimation Method for OFDM Systems with High Velocities,” In Proc. IEEE VTC, vol. 4, pp. 2358– 2361, 2003.
7. R. J. Lyman, “Decision-Directed Tracking of Fading Channels using Linear Prediction of the Fading Envelope,” in Proc. 1999 Asilomar Conf. Signal Process. Syst. Comput., vol. 2, pp. 1154–1158.
8. S. Kalyani and K. Giridhar, “Mitigation of Error Propagation in Decision-Directed OFDM Channel Tracking using Generalized Estimators,” IEEE Trans. Signal Process., vol. 55, no. 5, pp. 1659–1672, May 2007.
9. K.G. Wu and M.-K. C. Chang, “Adaptively Regularized Least-Squares Estimator for Decision-Directed Channel Estimation in Transmit-Diversity OFDM Systems,” IEEE Wireless Comm., vol. 3, No. 3, June 2014.

AN OVERVIEW ON WIRELESS BODY AREA NETWORKS IN MODERN MEDICAL AND HEALTH CARE SYSTEMS

K. Manasa[1]., B.Swathi[2]., B.Sharvani[3]., B.Sushmitha[4]., B.Praneetha[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: kondamanasa26@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0418, 15RG1A0419, 15RG1A0421, 15RG1A0422), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

***Abstract*— The increasing use of various new technologies related to wireless networks and the goal of improving the quality of life of cases for the development of wireless networks (WBANs). In WBAN, the variable type is appended or implemented in the body. This technology brings with it a new application called medical application. The purpose of the medical app is to collect sensitive data that will be used by the healthcare provider. Access of the health care provider to the resource for monitoring the condition of the property at any time of the day or night. Using these medical technologies and applications can reduce the cost of the medical application, and the healthcare provider can also monitor the objects remotely rather than face-to-face. This article focuses on the WBAN concept and the problems and challenges of open research are discussed for future studies.**

***Keywords*— Wireless Body Area Networks (WBANs), Body Area Networks (BANs), Security, Healthcare, Medical, Wireless networks.**

1. INTRODUCTION

The increasing use of various new technologies related to wireless networks and the goal of improving the quality of life of cases for the development of wireless body surface networks (WBANs). In the WBAN, the type of variable sensor (e.g. blood pressure, electroencephalography, called EEG, electrocardiogram (EKG), etc. (see Figure 1)) is attached or implemented in the body. These sensors can collect and transmit data to one another on a small and large scale. This technology brings with it a new application called medical application [1]. The purpose of the medical app is to collect sensitive data that will be used by the healthcare provider [2, 3]. Access of the health care provider to the resource for monitoring the condition of the property at any time of the day or night. The use of these technologies and medical applications helps reduce the cost of medical applications, and healthcare providers can also monitor objects remotely rather than face-to-face [4, 5].

WBANs can be connected to many wireless technologies like Rube, ZigBee, bluetooth type, etc. In this regard, this technology helps people move freely in different environments while the healthcare provider needs to access their health record in order to be able to monitor it remotely. This opportunity brings new challenges to the nature of WBAN and wireless technologies such as active and passive attacks [6].

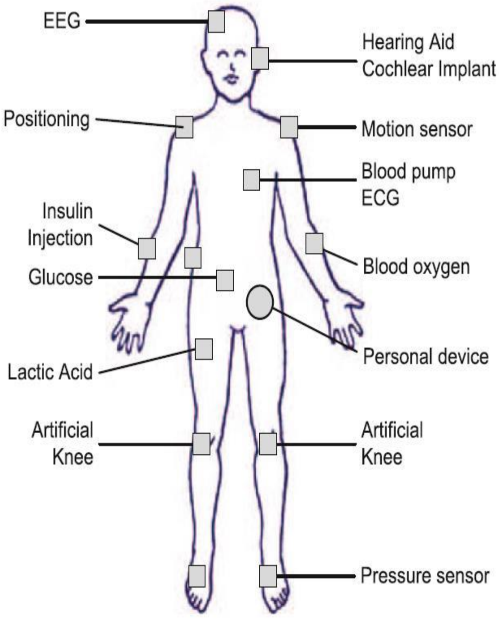


Figure 1: Sensor type in BAN

2. PROPOSED SYSTEM

The main applications of the wireless body network (WBAN) are the medical applications in which it is used in the healthcare sector. The example of this application is shown in Figure 1. As shown in Figure 1, the abundance sensor can be attached to the body or inserted under the skin [6-8]. These sensors collect important body data when the patient is in a different situation, e.g. B. in bed, while running, at work in the office, etc. [2, 9]. Additionally, the security domain is the other area where we can use WBAN to collect sensitive data and transmit the collected data to the server for other services . As explained in detail in [10], the use of health services is increasing in the USA, as shown in Figure 2.

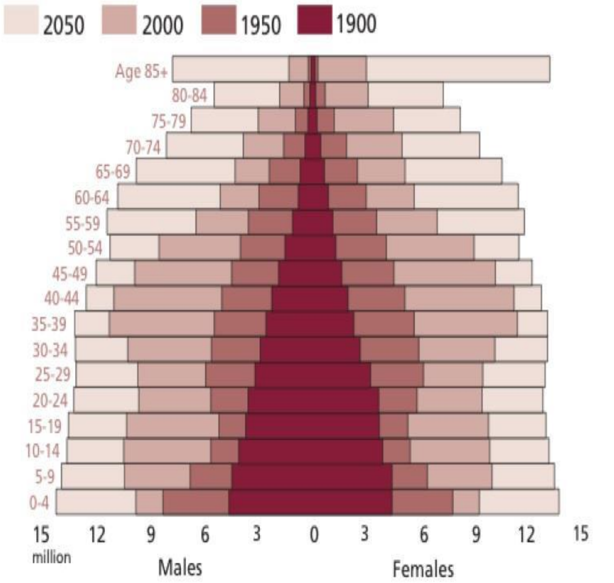


Figure 2: Age pyramid in the United States [10]

2.1 Device type in WBAN

Sensor Nodes - As we saw earlier, there are many sensors that are used to collect important data. This data is then transmitted to the next node called PDA (Personal Digital Assistance).

Personal Digital Assistance (PDA): PDA or other existing device, e.g. B. a smartphone, collects medical data from body sensors and processes them. The aggregated data is transmitted to the next hop, which is called the base station.

Base Station (BS) - There are many devices, e.g. B. Access points that act as switches in the network. The data is redirected from a local location to the cloud via the Internet. As a result, the medical data is stored on another server in the cloud or on any medical server in the hospitals.

2.2 Ease of use

The other major issue with WBANs is ease of use, which should be considered before implementing WBANs in both small and large areas. Regarding the characteristics of the WBAN and a large number of devices, including some variable sensors mounted or implemented in the body, as well as PDAs that collected data from the variable sensor, we need to provide a model to support them on both small and large scale. Also, due to the nature of WBAN, the patent makes it very easy to move from your location to another location or from your domain to another domain. As a result, there are many interactions between your communications that need to be considered before implementing WBANs. Figure 3 shows the location of the WBAN.

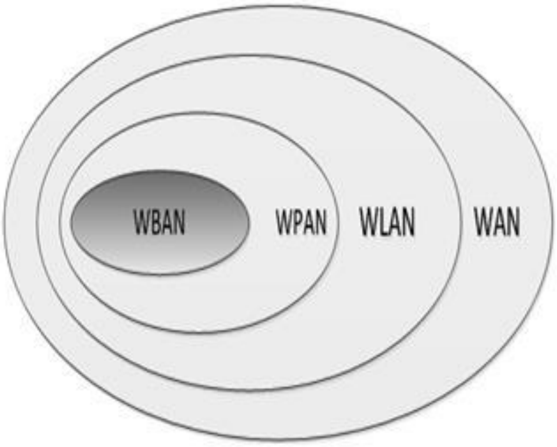


Figure 3: WBAN location

2.3 Security and Confidentiality

As explained above, due to the use of many devices such as variable sensors and PDAs, etc. sensitive medical data is transmitted over different types of wireless communication, what different challenges in terms of security and confidentiality with it brings. Researchers should consider data protection in WBANs to protect shared data from non-theoretical users. In addition, security mechanisms must be provided to ensure communication between and within WBANs in the same domain and in different domains. Many techniques related to security and privacy in WBANs are proposed to solve the existing problem, but we also need to focus more on the proposed effective techniques to meet the needs of WBANs [18]. Figure 4 shows the general wireless communication between WVBAs and their service providers.

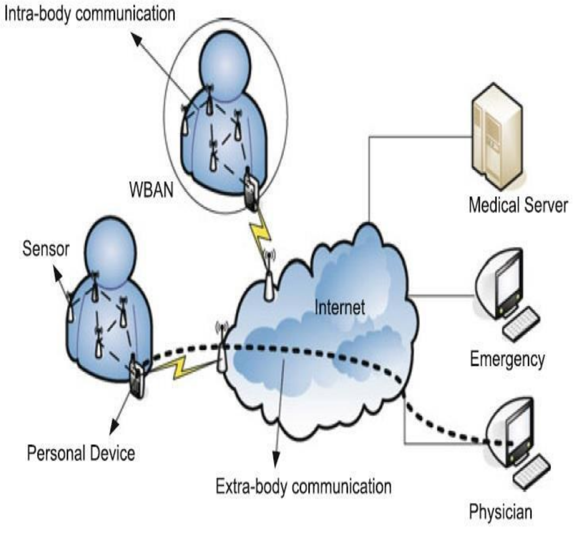


Figure 4: WBAN communication [8]

3. RESULT AND DISCUSSION

As discussed earlier in this article, sensitive data captured by body sensors is added to personal devices such as smartphones. And then the data is transferred to the medical cloud server and so on. In this regard, communication between and within WBANs can be broken down into three sections, on the one hand communication between sensors, called intra-communication, and on the other hand, communication between sensors and personal devices, called intercommunication. And the rest of the communication in the health networks is called beyond networks. As mentioned in the section on security, different security mechanisms are required for each communication layer. In addition, robust data protection and security techniques are required to meet WBAN and security requirements (see Figure 5). The type of wireless technology available is shown in Figure 6 with the data rate and frequency available.

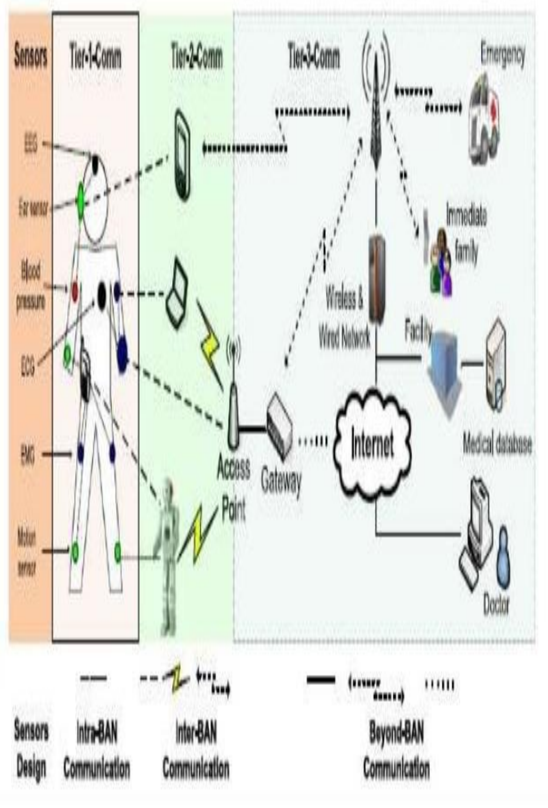
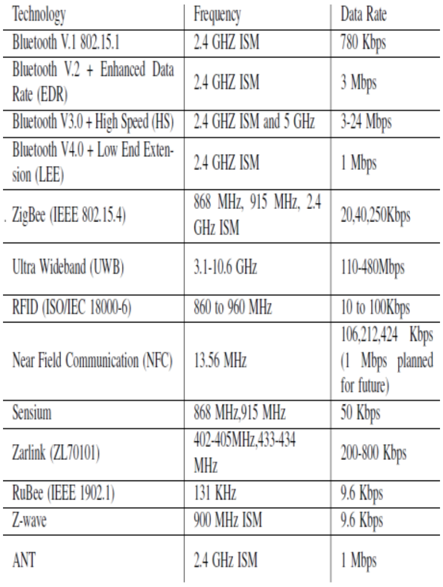


Figure 5: WBAN termination



Technology	Frequency	Data Rate
Bluetooth V.1 802.15.1	2.4 GHZ ISM	780 Kbps
Bluetooth V.2 + Enhanced Data Rate (EDR)	2.4 GHZ ISM	3 Mbps
Bluetooth V3.0 + High Speed (HS)	2.4 GHZ ISM and 5 GHz	3-24 Mbps
Bluetooth V4.0 + Low End Extension (LEE)	2.4 GHZ ISM	1 Mbps
. ZigBee (IEEE 802.15.4)	868 MHz, 915 MHz, 2.4 GHz ISM	20,40,250Kbps
Ultra Wideband (UWB)	3.1-10.6 GHz	110-480Mbps
RFID (ISO/IEC 18000-6)	860 to 960 MHz	10 to 100Kbps
Near Field Communication (NFC)	13.56 MHz	106,212,424 Kbps (1 Mbps planned for future)
Sensium	868 MHz,915 MHz	50 Kbps
Zarlink (ZL70101)	402-405MHz,433-434 MHz	200-800 Kbps
RuBee (IEEE 1902.1)	131 KHz	9.6 Kbps
Z-wave	900 MHz ISM	9.6 Kbps
ANT	2.4 GHz ISM	1 Mbps

Figure 6: Type of wireless technology in WBAN

3. WBAN applications and WBAN technologies

As mentioned earlier, the medical app is a promising app that improves the quality of life. While wireless communication over WBANs provides a platform for the transmission of data from the sensor to the medical server, wireless technologies are also important and should be considered before implementing networks. There are many wireless technologies such as IEEE 802.15.X that the researcher used in his model, but IEEE 802.15.6 is the best wireless technology that meets the main requirements of WBANs. Reliability, power consumption, data rate, latency, and physical layer security are some of the key characteristics of IEEE 802.15.6 that set it apart from others. Provision of strong security mechanisms between sensor nodes in BANs in order to be able to better use the security functions of the physical layer such as the wireless channel.

4. CONCLUSIONS

Wireless Body Area Networks (WBAN) is an emerging technology used in healthcare to improve the quality of life. In WBAN, the variable type is appended or implemented in the body. This technology brings with it a new application called medical application. The purpose of the medical app is to collect sensitive data that will be used by the healthcare provider. Access of the health care provider to the resource for monitoring the condition of the property at any time of the day or night. Using these medical technologies and applications can reduce the cost of the medical application, and the healthcare provider can also monitor the objects remotely rather than face-to-face. In this article, we will focus on the concept of WBAN.

REFERENCES

1. K. M. Pouryazdanpanah, M. Anjomshoa, S. A. Salehi, A. Afroozeh, and G. M. Moshfegh, "DS-VBF: Dual sink vector-based routing protocol for underwater wireless sensor network," in Control and System Graduate Research Colloquium (ICSGRC), 2014 IEEE 5th, 2014, pp. 227-232: IEEE.
2. M. Razzaque, A. Salehi, and S. M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: survey and the road ahead," in Wireless Networks and Security: Springer, 2013, pp. 107-132.
3. K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad hoc networks, vol. 3, no. 3, pp. 325-349, 2005.
4. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393-422, 2002.
5. Taparugssanagorn, A. Rabbachin, M. Hämäläinen, J. Saloranta, and J. Iinatti, "A review of channel modelling for wireless body area network in wireless medical communications," 2008.
6. S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in Space Science and Communication (IconSpace), 2013 IEEE International Conference on, 2013, pp. 361-365: IEEE.
7. S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: Issues and challanges," in Space Science and Communication (IconSpace), 2013 IEEE International Conference on, 2013, pp. 356-360: IEEE.
8. S. S. Ahmad, S. Camtepe, and D. Jayalath, "Understanding data flow and security requirements in wireless body area networks for healthcare," in E-health Networking.

REVIEW ON HIGH SPEED 32 POINT CYCLOTOMIC PARALLEL FFT PROCESSOR WITH PARALLEL FFT AND FFT TUBE COMBINATIONS

Dr.Selvamani Indrajith[1]., CH.Haritha[2]., H.Saisri[3]., D.Prathiba[4]., Ch.Harika[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: venkatasivareddy @gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0424, 15RG1A0425, 15RG1A0427, 15RG1A0426), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

***Abstract*— The parallel cyclotomic processor with fast Fourier transform (FFT) was introduced. The fast Fourier transform is one of the rudimentary operations in the field of digital signal and image processing. FFT is a technique that efficiently calculates DFT by reducing the number of addition and multiplication operations performed. Ciclotomic FFT is the type of FFT-DFT algorithm in various convolutions. This document shows the tradeoff between surface and performance. Cyclotomic FFT will help reduce this lag in FFT. This document focuses on the developments of the Radix-4 32-point FFT using VHDL as the design unit. Parallel FFT and FFT tube combinations are used to improve efficiency and speed. The results of the synthesis show the calculation used to calculate the FFT by VHDL and its performance. .**

***Keywords*— fast fourier transform (FFT), Radix, VHDL, Cyclotomic, Pipeline FFT, Butterfly, Parallel FFT**

1. INTRODUCTION

The FFT processor is widely used in mobile systems for signal and image processing applications. The need for low power FFT architectures for portable telecommunications systems is becoming increasingly important. Due to its nondisruptive sampling rate processing nature , the channelized FFT is the main architecture for high performance or low power solutions. In channelized architectures, the power consumption in each phase is dominated by the switch and the complex multiplier. This suggests the design of a 32 point FFT processing block. Project work focuses on the design and implementation of FFT. This design calculates the 32 point FFT and all numbers follow the fixed point format up to the frequency domain. Channelized FFT is seen as the primary architecture for real-time applications. However, the use of a single processor element (PE) in each stage limits the performance of channelized FFTs. Therefore, higher performance requires more parallelization.

2. LITERATURE REVIEW

This article, entitled "Analysis and Design of a Radix-4 Low Power FFT Processor Using a Channelized Architecture," proposes a low power technique for fast Fourier transform . This strategy for a fast Fourier transform is a high form of the discrete Fourier transform, with fewer calculations much easier, more efficient and faster is , as you master in various fields. Currently, the scope is limited to the 16-point channeled FFT processor for Radix-2 and Radix-4 implementations. Future research will include implementing a state-of-the-art FFT processor and evaluating another efficient architecture with the proposed architecture using low power techniques [1].

Article entitled "Fast Fourier Transform Design Using a Processing Element for True Value Signals" proposed in the Fast Fast Fourier Transform (IFFT) In-situ Computation Architecture for True Value Signals. The proposed calculation is based on the modified Radix-2 algorithm, which eliminates redundant flowchart operations. The modified flowchart contains only real data paths as opposed to complex data paths in a regular flowchart. A new processing element (PE) is proposed, which consists of two Radix-2 butterflies that can process four input signals in parallel. The number of calculation cycles is reduced by increasing the number of PE. Since redundant processes are eliminated, hardware costs are reduced [2].

This article, titled "Designing and Simulating a 32-Point FFT Using the Radix-2 Algorithm for FPGA Implementation," proposed for Fast Fourier Transform (FFT) is one of the basic operations on the Field of processing digital signals and images. Some of the major applications of Fast Fourier Transform include signal analysis, sound filtering, data compression, partial differential equations, large integer multiplication, image filtering, and so on. Fast Fourier Transform (FFT) is an efficient implementation of Discrete Fourier Transform (DFT).). It is the result of the given simulation that the input is applied, its 32 complex numbers. The output is in binary format and the output is in waveform [3].

The paper contains "Design and Implementation of Parallel FFT in CUDA". The Fast Fourier Transform (FFT) algorithm plays an important role in image processing and scientific computation, and is a division and a highly parallel conquest. The results show that the parallel FFT algorithm more efficient is than the ordinary FFT algorithm [4].

In this article, "High Performance, Low Power FFT Cores," ETRI Journal, integrated circuit power consumption has received increasing attention. Various combinations of low power hybrid technologies are used to reduce power consumption, e.g. these include, for example, multipliers that replace complex multipliers in FFTs, low power switches based on advanced interconnect architectures, and parallel pipeline architectures. Several FFT cores are implemented and evaluated to determine their performance and surface performance [5].

3. EXPERIMENTAL STUDY

The proposed methodology through which we will mention with the schematic diagram.

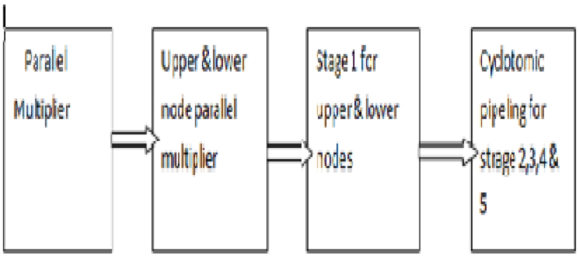

Paralel Multipler
Upper&lower node parallel multiplier
Stage 1 fcr upper&lower nodes
Cyclotomic pipeling for strage 2,3,4& 5

Fig. -1: Functional diagram of the proposed methodology

The first model of our project is a parallel multiplier, which is used to multiply complex numbers. Multiplication is one of the most important arithmetic functions, especially when implemented in programmable logic. The following figure shows the complex multiplier in the gallium field and the output waveform.

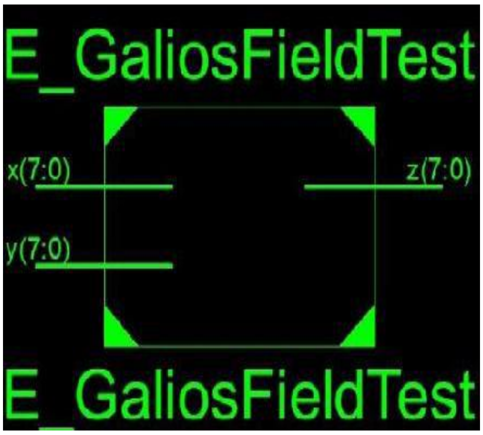


Figure -2: Galios field

4. RESULTS

FFT is a technique that efficiently calculates DFT by reducing the number of addition and multiplication operations performed. Ciclotomic FFT is the type of FFT-DFT algorithm in various convolutions. This document shows the tradeoff between surface and performance. Cyclotomic FFT will help reduce this lag in FFT. This document focuses on the developments of the Radix-4 32-point FFT using VHDL as the design unit. Parallel FFT and FFT tube combinations are used to improve efficiency and speed. The results of the synthesis show the calculation used to calculate the FFT by VHDL and its performance.

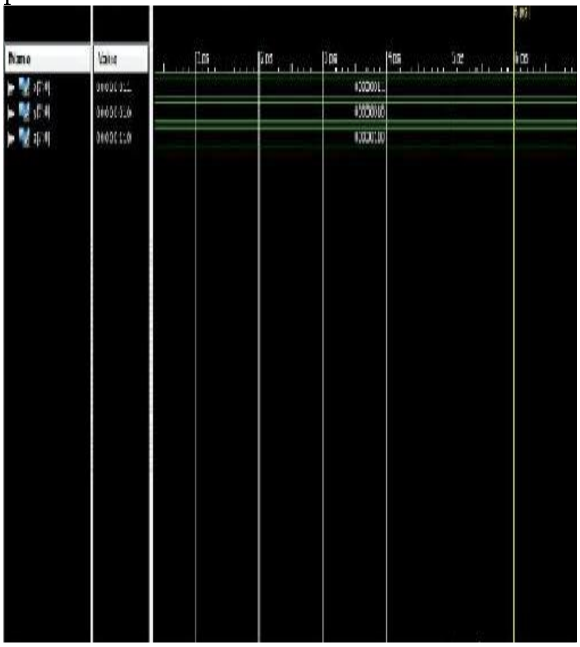


Fig. -3: The output of the complex multiplier

5. CONCLUSIONS

Transposition units to apply FFT also to the concept of FFT sound processing to generate IFFTs using FFT and reduce delay and power. The future scope is to extend the performance in the single clock cycle to improve the speed by five levels so that more than one operation can reduce the delay and performance. We can use parallel processing, it creates a large delay, and the power consumption is large. It must have a large number of multiplication and addition operations, so the operation using FFT needs a large delay because the multiplication method can be changed using algorithms.

REFERENCES

1. RuchiraShirbhate, TejaswiniPanse and ChetanRalekar," Design of Parallel FFT Architecture Using Cooley TukeyAlgorithm",This full-text paper was peer-reviewed and accepted to be presented at the IEEE ICCSP 2015 conference.
2. Afreen Fatima , "Designing and Simulation of 32 Point Fft Using Radix-2 Algorithm for Fpga", Department : Electronics Affiliated To : JNTU (HYD).
3. SharadSingh,MrsJyotiKedia, "Pipelined FFT Architectures: A Review",-978-1-4799-7678-2/15/$3100.Elecrical, Electronics, Signals, Communication and optimization(EESCO),2015 International conference on©2015 IEEE.
4. Mohammed A. El-Motaz, Ahmed M. El-Shafiey, Mohamed E. Farag,"Speeding-up Fast Fourier Transform",2015 IEEE International conference on Electronics, Circuits and systems(ICECS9)78-1-5090-0246-7/15/$31.00 ©2015 IEEE 510.
5. WeihuaZheng, Kenli Li, Member, KeqinLi,Hing Cheung So, "A Modified Multiple Alignment Fast FourierTransform with Higher Efficiency". 10.1109/TCBB.2016.2530064, IEEE/ACM Transactions on Computational Biology and Bioinformatics.
6. Wei Han, Ahmet T. Erdogan, Tughrul Arslan, and Mohd. Hasan, "High-Performance Low-Power FFT Cores",ETRI Journal, Volume 30, Number 3, June 2008.
7. Shymna Nizar, N.S,Abhila, R Krishna, "An Efficient Folded Pipelined Architecture For Fast Fourier Transform Using Cordie Algorithm", 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (lCACCCT).

REDUCTION OF END TO END DELAY IN MANET USING CLUSTER BASED ADAPTIVE BROADCASTING SCHEME

CH.Keerthi[1]., D.Swetha[2]., K.Swetha[3]., D.Sushmitha[4]., D.Vinitha[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: keerthureddychinthala@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0429, 15RG1A0430, 15RG1A0431, 15RG1A0432), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— Mobile Ad Hoc Network (MANET) has a distributed and decentralized architecture with mobile nodes. Since the nodes are mobile in nature, it is difficult to maintain the route and connection between the origin and the destination. The routing process increases routing overhead and decreases performance due to the large routing table used by mobile nodes. To solve this problem, various approaches are being developed to make routing more efficient. However, they didn't focus on the connection errors and path errors. We propose an Adaptive Cluster-Based Transmission (CBAB) scheme to strike the right balance between end-to-end congestion and delay. In the first phase of this diagram, we create the cluster routing procedure and cluster head selection based on the neighbour coverage metric. In the second phase, the overhead is reduced thanks to the connection time-out and the elimination of redundant retransmission messages. The simulation results show that the proposed scheme achieves a better handover rate, a lower communication overload, a lower control overload, a lower computational effort and a very low end-to-end delay than the existing schemes, namely the AODV and Dynamic Route Discovery (RRD).

***Keywords*— MANET, Cluster, overhead reduction, delivery ratio, control overhead, and end to end delay.**

1. INTRODUCTION

Mobile ad hoc networks (MANET) have become an active research area in recent years. MANETs consist of wireless hosts that communicate with each other without a fixed infrastructure. The nodes of a MANET exchange information via peer-to-peer routes with one and more hops. Collaborative computing and communication in smaller areas can be configured using ad hoc network technologies. The task of route maintenance in MANET is important because mobile host nodes cause frequent random topological changes. Many routing protocols, such as on-demand ad hoc distance vector routing (AODV) [1] and dynamic source routing (DSR) [2], have been proposed for MANET. These protocols are based on on-demand routing and can be used to improve the scalability of MANETs by reducing the routing overhead [3]. AODV is the most popular algorithm that can be used and is suitable for MANET routing with a minimal number of nodes. Minimal delay is required in path configuration and wired networks can be used in MANET with fewer disruptions.

2. RELATED WORKS

Aggregation approaches generally fall into six categories. Mobility-based clustering approaches, clustering approaches based on common metrics; Mastery of set-based clustering approaches, energy-efficient clustering approaches, load balancing clustering approaches and low-maintenance clustering approaches [6]. For this situation, an energy efficient clustering approach is used that avoids unnecessary power consumption or balanced power consumption for nodes in mobile ad hoc networks in order to maintain the network longevity, i. H. - For example, the lifetime of mobile nodes. In the location-based scheme, messages are only forwarded if the concept of additional coverage [7] determines the location of the mobile nodes to be sent. In the distance-based scheme, messages are forwarded based on the decision made between the relative distance of the mobile node and the previous sender. In the cluster-based scheme, the network is divided into several clusters. Hybrid schemes [8] combine the advantages of opposing schemes and probabilistic schemes to improve performance. The second category is known as the deterministic broadcast scheme and includes multipoint handover [9], node handover [10], neighbor deletion [11], and clustering [12]. The solutions suggest that under the traditional back pressure algorithm, in which the end-to-end delay of packets first decreases the network load or the arrival rate and then increases it occasionally [13].

3. PROPOSED WORK

The proposed scheme has two phases. In the first phase, a hybrid clustering algorithm is developed that is based on the metric of the neighbor coverage. In this phase the group model is designed and the group leader is selected based on the initial group value. In the second phase of the diagram, the connection stability estimate is determined in order to reduce redundant messages, which leads to a reduced overhead. These phases of the proposed routing scheme are described below. The detailed steps are shown in Figure 1.

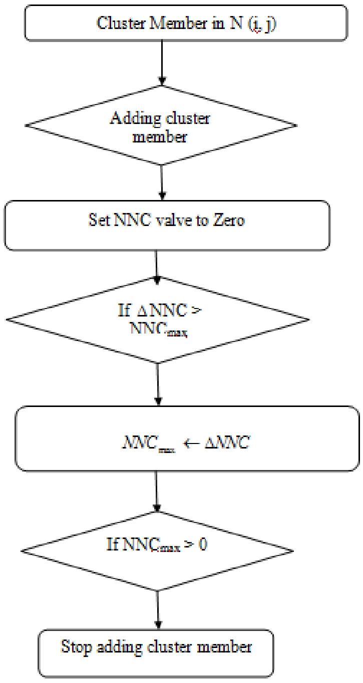


Fig. -1: Flow diagram of the proposed grouping scheme

In this phase, the cluster is formed from the group of mobile nodes based on the coverage of neighboring nodes (NNC). The current cluster adds all neighboring mobile nodes, resulting in a positive NNC gain for nodes already in the cluster.

$$Aij(t) = \begin{cases} 0 & i \leftrightarrow j \; notconnected \\ 1 & i \leftrightarrow j \quad Connected \end{cases}$$

Aij (t) has the Markov property. Link connectivity is mainly affected by the characteristics of the radio channel when the two nodes are fixed or moving at a relatively slow speed. The probability of receiving a packet incorrectly is usually indicated by the probability of error, which is independent of whether the previous packet was received successfully. Let tp be the current moment, the probability of the connection stability is assessed if the connection remains connected for the time k,

$$Gr(k) = G\{s_{10} > k\} = e^{-\mu(tp)k}$$

3.1 Proposed algorithm to reduce overhead

The overhead reduction algorithm is explained in the following steps:

i) The originating node sends a route request to all nodes within range. The receiving node checks the correct replication or order.
ii) If this is correct, it checks whether it can provide the requested data, otherwise it marks its own address and sequence number on the request packet and retransmits the packet.
iii) A new route detection is started before the connection expires.
iv) Set a maximum lifetime for packets to minimize transmission overhead and control traffic.
v) By reducing the control traffic, more traffic can be transmitted over the network. For example let

4. PERFORMANCE ANALYSIS

This section evaluates the performance of the proposed approach. The simulation model is discussed and the simulation results are presented and described below. We simulated our results with the simulator ns 2.34 . Here we assume that all nodes adopted for the simulation move dynamically, including the direction and speed of the nodes. The mobility scenario is generated using a random waypoint model with 300 nodes in an area of 900 m × 900 m. The simulation parameters are listed in Table 1 below.

The performance of any algorithm can be assessed using the following metrics.

Package delivery rate: The package delivery rate is defined as the ratio of the number of packets sent by sources at a constant rate to the number of packets received at the destination. The best routing methods that use this metric are those that ensure delivery that guarantees message delivery by assuming a "reasonably" accurate neighboring destination and location with no message collision.

Control Overload: Control Overload is defined as the total number of normalized routing control packets multiplied by the total number of data packets received. The overload of the control traffic of a protocol is strongly related to the stability of the connectivity graph in MANET.

Routing congestion: The overhead associated with QoS routing is a major constraint on your implementation. In simple terms, the flooding process used to distribute network status is a major contributing factor to QoS routing congestion. The mechanisms for overcoming the cost of QoS routing, e.g. B. those that limit the frequency of issuing updates, create new problems, namely the inaccuracy of routing information.

End-to-End Delay - This is also known as latency and is the time it takes for the message to be delivered. The data delay can be divided into queue delay and propagation delay. If the queue delay is ignored, the propagation delay can be replaced by the number of hops due to the proportionality.

The simulation parameters and parameters are summarized in Table 1.

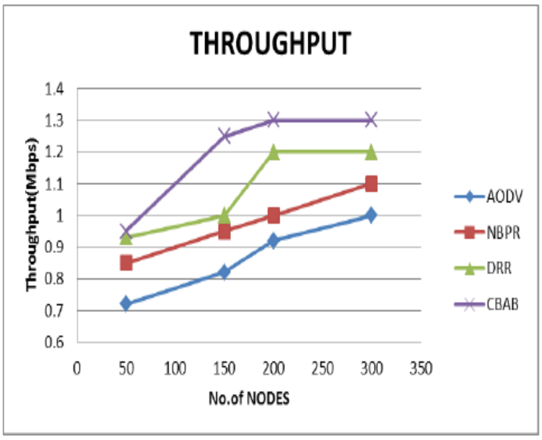
Table 1: Simulation and configuration parameters

No. of Nodes	300
Area Size	900 X 900
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	128 bytes
Mobility Model	Random Way Point
Protocol	AODV

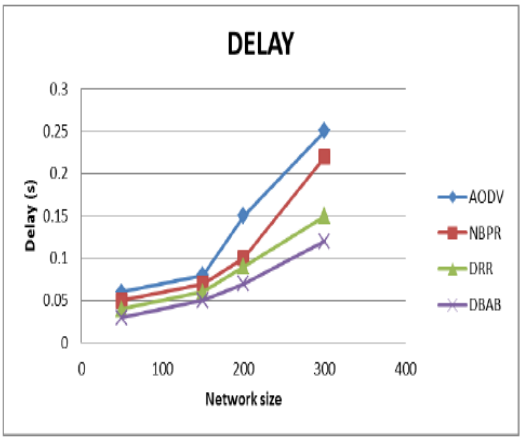
5. RESULTS

We compare our proposed CBAB scheme to AODV, Neighbor Based Probabilistic Relay (NBPR), and Dynamic Route Discovery (DRR). The results are examined using performance metrics, end-to-end delay, packet delivery percentages, and control overload. By varying the network size and performance parameters, the packet delivery rate, control load and delay are analyzed using trace analysis. It is clearly shown that the network varies from 60 nodes to 300 nodes. He analyzed the four parameters using existing and proposed protocols with different mobility conditions. The theoretical

maximum throughput is closely related to the channel capacity of the system and is the maximum possible amount of data that can be transferred under ideal circumstances.



Graph -1: Graphical comparison in terms of performance



Graph -2: Graphical comparison with regard to the delay

In Figure 3, the performance of CBAB is compared to other techniques and in particular the execution rate is compared. The network using the CBAB protocol has a high delivery and packet rate.

In Figure 5, the performance of networks using the AODV protocol is compared to another protocol, and more specifically, the routing overhead is compared. The network using the NBPR protocol has less overhead and CBAB has a high routing overhead.

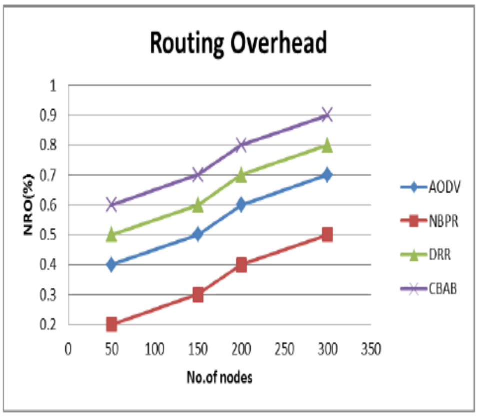


Diagram -5: Graphical analysis of the routing overhead

5. CONCLUSION

We offer the Adaptive Cluster Transmission (CBAB) scheme to find the right balance between overhead and end-to-end delays. In the first phase of this diagram, we create the cluster routing procedure and cluster header selection based on the neighbor coverage metric. In the second phase, the overhead was reduced through connection timeouts and the elimination of redundant relay messages. By implementing these solutions, we have achieved better stability and less overhead for the ultimate goal of the cluster routing scheme. The proposed work may be an approach that suggests a real world approach, such as B. Military search and rescue operations. Future studies can be expanded to implement power consumption with a layered framework in the routing scheme for stable connections to achieve minimal power consumption between mobile nodes.

REFERENCES

1. N. Karthikeyan, V. Palanisamy and K. Duraiswamy, “Reducing Broadcast Overhead Using Clustering Based Broadcast Mechanism in Mobile Ad Hoc Network”, Journal of Computer Science 5 (8): 548-556, 2009.
2. Xin Ming Zhang, Member, IEEE, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, Senior Member, IEEE, “An Estimated Distance-Based Routing Protocol for Mobile Ad hoc Networks”, IEEE Transactions on Vehicular Technology, Vol. 60, No. 7, September 2011, pp.3473-3484.
3. Narendra Singh Yadav, Bhaskar P Deosarkar and R.P.Yadav, “A Low Control Overhead Cluster Maintenance Scheme for Mobile Ad hoc NETworks (MANETs)”, International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009, pp.100-104.
4. Ha Dang, Member, IEEE, and Hongyi Wu, Member, IEEE, “Clustering and Cluster-Based Routing rotocol for Delay-Tolerant Mobile Networks”, IEEE Transactions on Wireless Communications, Vol. 9, No. 6, June 2010, pp.1874-1881.
5. Samer A. B. Awwad, Chee Kyun Ng* and Nor K. Noordin, “Cluster Based Routing Protocol with Adaptive Scheduling for Mobility and Energy Awareness in Wireless Sensor Network”, Proceedings of the Asia-Pacific Advanced Network 2010 v. 30, p. 57-65.
6. Dr.G.Mary Jansi Rani and Dr. S. Arumugam, “Control overhead reduction: A Hierarchical Routing Protocol in Mobile Ad hoc Networks”, International Journal on Computer Science and Engineering, Vol.5, No.5, 5, No.5, 2013, pp.275-279.
7. J. Cartigny, D. Simplot, Border node retransmission based probabilistic broadcast protocols in ad-hoc networks, in: Proceedings of HICSS-36, 2003.

DESIGN AND IMPLEMENTATION OF AUTONOMOUS AMPHIBIOUS UNMANNED AERIAL VEHICLE FOR NAVIGATION AND SAFE LANDING OVER WATER

Ch. Mahesh[1]., E.Pavani[2]., G.Sravanthi[3]., G.Anusha[4]., G.Srivani[5]

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉@: mahesh@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0433, 15RG1A0434, 15RG1A0435, 15RG1A0436), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Automatic landing system for Autonomous Amphibious Unmanned Aerial Vehicle (AAUAV) hovering on water surface is proposed. AAUAV comprises of inculcating multicopter and hover craft configurations to be served as an aerial vehicle as well as hovering on water bodies. The placement of hovercraft on the water surface, after the multicopter carries the hovercraft as a payload to the particular location in water, has to be done precisely so as to keep the vehicle safe from getting into the water. For this purpose, the propulsion system of the multicopter and the hovercraft are controlled with an aid of information from Ultrasonic sensor. The distance above the water surface is measured using ultrasonic sensor and after a threshold level of distance, a control signal from Arduino will be sent to respective brushless DC motors of both the configurations to hover the vehicle above the water surface. Preliminary experiments are conducted and test results confirmed that the developed control will be utilized in controlling AAUAV for water sampling applications..

Keywords— Amphibian uav, multicopter, hovercraft, arduino, ultrasonic detector, autopilot

1. INTRODUCTION

Two separate vehicles were assumed for the AAUAV (Amphibious Unmanned Autonomous Aerial Vehicle). One hovercraft and the other is a multicopter . They are both flexible in terms of adhesion and breakage. This shows that it can be used separately as a multicopter and hovercraft if needed. The main task of being an autonomous amphibious drone must unite the two. In flight at a certain point in time, the hovercraft is considered to be the payload of the multicopter. The increasing use of unmanned flight systems has forced the addition of precise techniques and technologies to the vehicle so that collisions due to obstacles in the way can be easily avoided while the mission route is carried out autonomously. For this purpose, sensors such as ultrasonic detector, laser rangefinder, etc. are used i . The same type of sensor can be selected from the group of options and used to identify and receive notifications of the hovercraft's position on the water surface, carefully handling this AAUAV vehicle.

The capabilities of laser sensors are far superior to the capabilities of ultrasonic sensors. However, ultrasonic sensors are able to provide an accurate reading when perpendicular or nearly perpendicular to the surface, making them a practical solution for measuring distance with the above items - above and below the quadcopter , being either of these objects is grounded, meaning this that the sensor can be used to determine the flight altitude up to the approach to the landing zone measure . The solution to the above difficulty can be overcome by using the ultrasonic detector with Arduino. In addition to sensing the distance above the water, you can turn the hovercraft lift motor on and off and rotate the multicóptero motors , respectively ,
to make the hovercraft run at the right time, resulting in a hovercraft perfectly suspended from the surface of the water.

2. PROPOSED SYSTEM

Unmanned autonomous amphibious aircraft system.The advantage AAUAV is , that in general, the can be used water as well as antenna applications, can be achieved by means of unmanned aircraft. AAUAVs differ significantly in the way they work from other normal drones. The application to be worked on with the help of AAUAV includes water analysis, water sampling, water research, delivery and monitoring of cargo, and much more. For these applications, a multicopter and hovercraft can be used together to complete a mission. . The two hovercraft and multicopters , can easily be separated and operated according to the requirements according to the shipment.

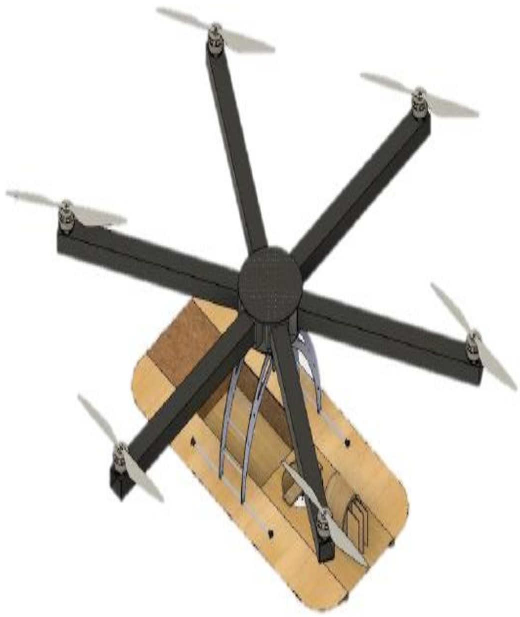


Figure 1 - 3D layout of AAUAV (hovercraft plus multicopter)

The multicopter used here is a hexacopter (with six Bldc motors) and can be modeled with carbon fibers due to its low weight and high strength. The middle section contains all the electronics and the multicopter landing gear is designed so that it can be attached to the top of the hovercraft with certain accessories. The hovercraft with the multicopter can travel far and be used in the water by flying from point to point in the mission application if necessary (if the hovercraft has to travel a long distance).

3. AAUAV CONTROL BY ARDUINO AND AUTOPILOT SYSTEM

3.1. Controlling Motors with Arduino

If the Arduino is programmed for a Bldc motor , it can operate and control more than one Bldc motor at the same time . This can be achieved by connecting the Arduino to the motor through a dedicated connection with the controller and connecting a battery to the controller to start the motor. The motor is connected to the ESC output. The connection was established as shown in Figure 2.

3.1.1. Controlling a motor with Arduino

In the case of a motor control with Arduino Uno, the connection between the Arduino Uno and the motor is established using the electronic speed controller (ESC) and thus the ESC connected to the battery. The following program is loaded onto the Arduino Uno while the motor is plugged into the lift shaft of one of the hovercraft prototype models.

The connection steps for connecting a single motor are as follows:

1. Program Arduino with Arduino IDE
2. Connect the motor to the ESC output
3. Connect the brown wire with the 3-pin cable that comes out of the controller to the "GND" pin of the Arduino .
4. Connect the yellow wire to any digital pin on the Arduino . We connect it to digital pin 12.
5. Connect the cables "+" and "-" of the battery with the cables "+" and "-" of the control unit.
6. Turn on the Arduino by connecting the cable to the computer / laptop and Arduino .
7. Download the program to the Arduino board . Iv

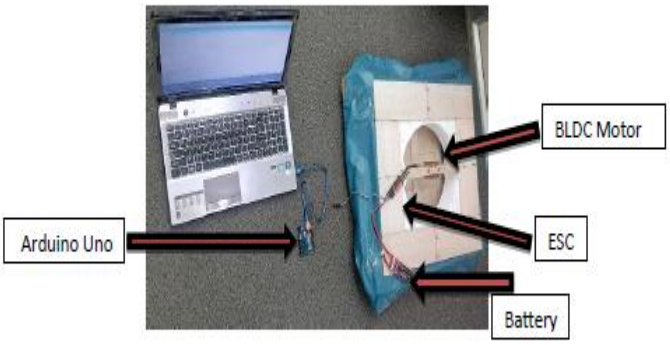


Figure2 - Arduino connection to the motor

3.2. Controlling AAUAV motors with Arduino

The Arduino board , as will be described for controlling an engine may, for simultaneous multiple motors used control are .

3.2.1. Explanation of the program

1. During the initialization, 7 servo objects (ie ESC) were created because we need to control 7 motors and can control different servos at the same time. Both ultrasound machines have pens, an echo, and a trigger pen. They have been plugged in and set to Arduino . The maximum and minimum distance were initialized by defining the duration and the distance.

2. The setup contains the definition of the servo connections and transmits the acoustic signals after a delay of 3 seconds each. In

addition , the set trigger in the settings helps us to get information about the distance.

3. In the loop, the sensor first switches itself on and off for a while. The equation distance = (duration / 2) / 29.1; It needs to be added to calculate or convert the speed of sound in air in terms of duration in centimeters . You have to cut it in half when traveling from side to side.

4. In the moment in which the ultrasonic cm distance of less than 60 according to the Arduino programming recognizes and calculates, turns the hoist motor of the hovercraft a to produce the air pressure in the interior of the skirt, it being liable to float can . in the water without being faced with a landing error. In the second step of this process , the Arduino switches off the 6 motors of the hexacopter when the ultrasound determines that the distance is 16 cm. In this sinking time of 60 cm to 16 cm, the hovercraft has enough time to obtain the required or maximum air pressure to float on the water.

4. RESULT AND DISCUSSION

The other way to control the motor for a safe landing is to connect the Arduino to the autopilot. In this case the motors are connected to the ESC and the motor and finally to the autopilot. While this autopilot connects to the Arduino . The ultrasonic sensor connected to the Arduino sends information about the height of the vehicle. As with the removal described in the previous program, the same distance is maintained. But the concept of control changes here. Thus receives the Arduino the information as soon as the distance between the vehicle and the water surface is 60 cm. When it decreases by two inches, the Arduino sends information to power the hovercraft motor. This continues until the distance is less than 60 cm and more than 16 cm from the water surface. If the distance falls below 16 cm, the Multicóptero's motor will stop. All of these controls are performed using information ultrasonically fed to the Arduino and therefore sent to the autopilot system to which the motors and all other controls are connected.

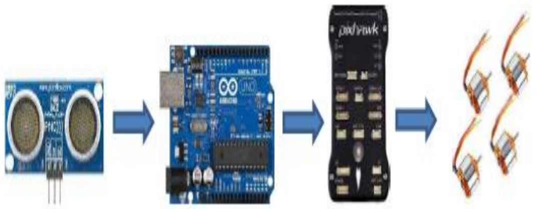


Figure 3 - Block diagram of the connection between the Arduino and the autopilot

The above diagram shows the connection that connects the ultrasonic sensor to the Arduino via its 3-pin connection, namely. Ground, Vcc and signal. The output from the arduino is going to be, on the broadcast Pixhawk autopilot , one has pre-programmed and calibrated engine stability function. This will connect and program all of the motors to be controlled according to the information sent to the Arduino and Pixhawk by the ultrasonic sensors .

5. CONCLUSION

The transition from multicopter mode to the hovercraft configuration of an amphibious vehicle for swimming along bodies of water is accomplished by controlling the motors of the particular configuration. As a threshold value of the ultrasonic sensor is a typical distance of 160 mm set and triggered the drive system. A simple floating ship is developed and the system is controlled with Arduino. The test result shows that the algorithm developed is used to control AAUAV effectively. Autopilot integration to achieve multi-mode AAUAV configurations is implemented in real-time water sampling applications to collect water samples and perform on-site water quality analysis.

REFERENCES

1. Nils Gageik, Thilo Muller, Sergio Montenegro: Obstacle detection and collision avoidance using ultrasonic distance sensors for an autonomous multicopter.
2. Pandya Garvit Kalpesh, "Distant mission UAV capability with on-path charging to increase endurance, on-board obstacle avoidance and route re-planning facility", International Journal of Computer Engineering in Research Trends, 4(1):10-14, January 2017. [Innospace-2017: Special Edition]
3. www.griffonhoverwork.com/whyhovercraft

4. https://www.instructables.com/id/Interfacing-Brushless-DC-Motor-BLDC-With-Arduino/
5. Anurag Singh Rajpoot, Namrata Gadani and Sagar Kalathia, “Development of Arduino based Quadcopter”, International Advanced Research Journal in Science, Engineering and Technology, Vol. 3, Issue 6, June 2016.

ACTIVE INTEGRATED MICROSTRIP ANTENNA SLITS WITH ENGRAVED HARMONIC SUPPRESSION GROOVES USING FR4 SUBSTRATE FOR WLAN

Dr.Archek Praveen Kumar[1]., G.Mandira[2]., G.Sravani[3]., G.Sirisha[4]., G.Shirisha[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: archekpraveen@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0437, 15RG1A0438, 15RG1A0439, 15RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

*Abstract***— *This article introduces and discusses a new active integrated microstrip antenna (AIA) design that is similar to a patch slot. The primary design passive antenna supports WiFi bands of 2.45 GHz. The antenna with harmonic suppression function is built directly into an amplifier to improve energy efficiency. The antenna is a microstrip field with engraved harmonic suppression grooves. The proposed passive patch antenna is integrated in a power amplifier (PA). The antenna was constructed with a substrate dielectric constant FR4 4.4 and a thickness h = 1.53 mm and had dimensions of 64.0 mm × 73.0 mm × 1.6 mm. The proposed antenna has a much higher impedance bandwidth (2.30-2.66 GHz) of about 15.33% (S11 <-10 dB) and the gain is about 3.4 dB. The radiation pattern, return loss, VSWR and bandwidth of the proposed antenna are described. and simulated with the HFSS software package..***

Keywords— microwave amplifiers; active integrated antenna slits, active components.

1. INTRODUCTION

In recent years, the active integrated antenna (AIA) aspect has become a growing and developing area of research that has received a lot of attention. In one definition, the AIA can be viewed as an active microwave circuit, the input or output of which ends in free space rather than conventional connections. The active device in an AIA can be of any type such as transistors (three terminal device), or resistors, inductors, and any flat antenna such as microstrip patch or microstrip slot antennas can be used as the radiating element.

2. LITERATURE SURVEY

The active integrated antenna (AIA) is a direct integration between an antenna and an active circuit such as a power amplifier (PA), a low noise amplifier (LNA) or an oscillator [1]. Such integration not only offers a reduced circuit size by reducing the number of circuit parts, but also improves the performance of the power amplifier when the antenna is designed to have a harmonic suppression capability [2]. The harmonic suppression antenna was constructed using shorting pins, circular sector antennas, photonic band gap (PBG) structures, and faulty ground [8]. Although these designs show good overall energy efficiency (EAP) improvement, the design is relatively complicated. This article introduces a simple square antenna design that may be modified to support both linear and circular polarization for practical communication interfaces [6]. This architecture is easy to manufacture compared to the short-circuit pin structure. The symmetrical geometry is another advantage that makes the antenna suitable for future circular polarization applications [7].

3. PROPOSED DESIGN AND ANALYSIS OF ANTENNAS

The dielectric chosen is an FR4 epoxy substrate with a relative permittivity of 4.4 and a thickness of 1.53 mm. The patch size is approximated using the basic design approach described for the microstrip patch antenna as follows:

Step 1: Compute Lambda (λ0) -
Lambda (λ0) = c / f = 3 x 10- & sup8; / 2.4 x 10- ?
(λ0) = 125 mm at 2.4 GHz

Step 2: calculate the length of the monopole (L) -

The operating frequency of the patch antenna is determined by the length L.

The center frequency is roughly given by:

$$f_c \approx \frac{c}{2L\sqrt{\varepsilon_r}}$$

$$L = \frac{C}{2fc\sqrt{\varepsilon_r}}$$

Hence we get W = 2.84 mm.

$$Z_0 = \frac{60}{\sqrt{\varepsilon_r}} \ln\left(8\left(\frac{H}{W}\right) + 0.25\left(\frac{W}{H}\right)\right)$$

3.1 Active integrated circuit:

With an active integrated antenna, the designed patch antenna should be connected directly to the output of the amplifier as a load. The input impedance of the antenna can be used as the RLC load in the HFSS simulation.

After designing the appropriate arrays for the input and output ports that will provide maximum gain while considering the stability of the amplifier, the next part is the DC bias circuit. This circuit must be able to isolate the RF sections of the amplifier from the DC parts. It should also be able to deliver the required DC power with minimal power dissipation as we are interested in an efficient design. The width of this transmission line must be very narrow to increase its characteristic impedance and the length must be a quarter wavelength. At the level of the amplifier, the frequency. Surgery.

On the other side of this narrow transmission line that the DC power supply is connected to, the use of some decoupling capacitors at this point effectively shorts all frequencies except the DC power supply. The quarter-wave transmission line converts the short circuit into an open circuit by connecting it to the amplifier network. This means that the input or output signals cannot propagate in this part of the circuit and in this way the RF network is isolated from the DC circuit. A simplified diagram for Integrated Active (HF and DC sections) is shown in Fig. 1. With an active antenna, the designed patch antenna should be connected directly to the output of the amplifier as a load. The input impedance of the antenna can be used as the RLC load in the HFSS simulation.

After designing the appropriate arrays for the input and output ports that will provide maximum gain while considering the stability of the amplifier, the next part is the DC bias circuit. This circuit must be able to isolate the RF sections of the amplifier from the DC parts. It should also be able to deliver the required DC power with minimal power dissipation as we are interested in an efficient design. The width of this transmission line must be very narrow to increase its characteristic impedance and the length must be a quarter wavelength. At the level of the amplifier, the frequency. Surgery.

On the other side of this narrow transmission line to which the DC power supply is connected, the use of certain decoupling capacitors at this point effectively shorts all frequencies with the exception of the DC power supply. The quarter-wave transmission line converts the short circuit into an open circuit by connecting it to the amplifier network. This means that the input or output signals cannot propagate in this part of the circuit and in this way the RF network is isolated from the DC circuit. A simplified diagram for Active Integrated (HF and DC sections) is shown in Fig. 2.

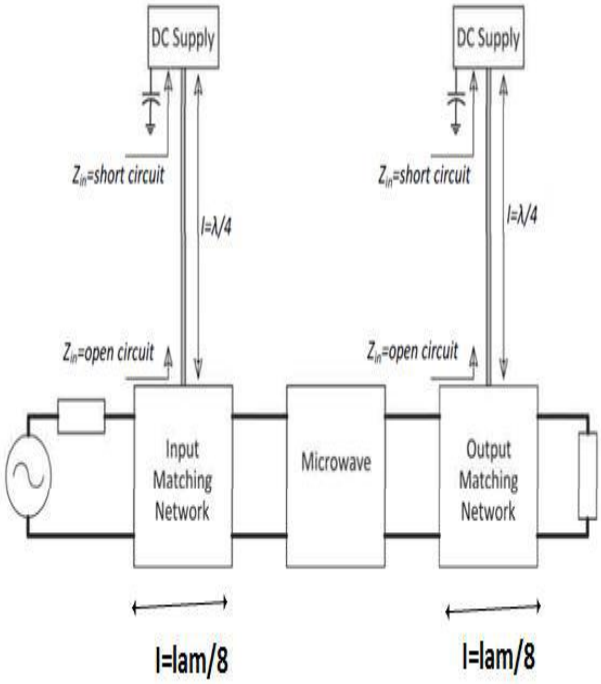


Fig 1: Active integrated circuit

2. Comparison table

Sr. No .	Results	Freq (GHz)	Return Loss (dB)	VSWR	BW MHz	Impedance
1.	Simulated Results	2.46	-16.55	1.34	300	52.2
2.	Measured Results	2.43	-33.43	1.03	320	51.1

4. RESULT ANALYSIS

The antenna was constructed with a substrate dielectric constant FR4 4.4 and a thickness h = 1.53 mm and had dimensions of 64.0 mm × 73.0 mm × 1.6 mm. The proposed antenna has a much higher impedance bandwidth (2.30-2.66 GHz) of about 15.33% (S11 <-10 dB) and the gain is about 3.4 dB. The radiation pattern, return loss, VSWR and bandwidth of the proposed antenna are described. and simulated with the HFSS software package.

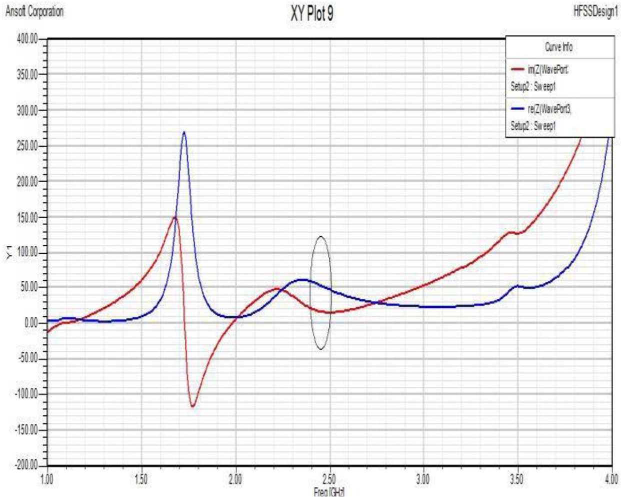


Fig 2: Active integrated antenna with harmonic suppression

The simulated passive antenna has frequency bands operating at 2.46 GHz and improved bandwidth levels are achieved by active amplifiers built into its ports. The simulated results for the proposed AIA show that it covers frequency bands from 2.30 to 2.66 GHz and, in contrast to the passive antenna, has an improvement in gain and bandwidth of 3.4 dB.

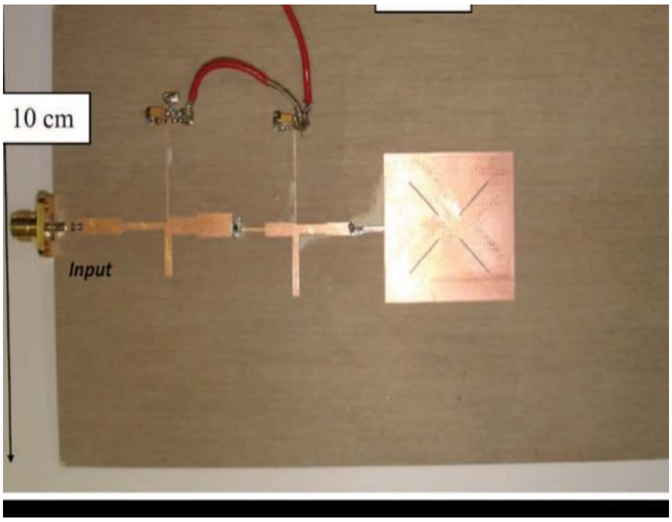


Figure 3: Antenna input impedance with harmonic suppression

5. CONCLUSION

In this work a new microstrip design with an integrated active slot antenna for WLAN applications is proposed. The simulated passive antenna has frequency bands operating at 2.46 GHz and improved bandwidth levels are achieved by active amplifiers built into its ports. The simulated results for the proposed AIA show that it covers frequency bands from 2.30 to 2.66 GHz and, in contrast to the passive antenna, has an improvement in gain and bandwidth of 3.4 dB. The measured and simulated results for the proposed active and passive antennas correlate and agree appropriately, and the proposed antenna can be used as an antenna for WLAN applications.

REFERENCES

1. H. Kim and Y. J. Yoon, “Wideband design of the fully integrated transmitter front-end with high power-added efficiency,” Microwave Theory and Techniques, IEEE Transactions on, vol. 55, no. 5, pp. 916–924,May 2007.
2. H. Kim and Y. J. Yoon, “Microstrip- fed slot antennas with suppressed harmonics," Antennas and Propagation, IEEE Transactions on, vol. 53, no. 9, pp. 2809–2817, 2005.
3. Ali Khoshniat and Reyhan Baktur, “A Linearly Polarized Active Integrated Square Microstrip Patch Antenna” IEEE Transactions on, vol. 9, no. 1, pp. 13–15,June2011.
4. Y.Park,S.-M.Han,and T.Itoh,”A rectenna design with Harmonic rejecting circular-sector antenna,” Antennas and Wireless Propagation Letters,IEEE Transactions,2004.
5. Horii and M.Tsutsumi,”Harmonic control by photonic bandgap on microstrip patch antenna, ”Microwave and Guided wave Letters, IEEE Transactions,vol.9,no.1,pp,13-15,Jan.1999.
6. Sung, M. Kim, and Y.Kim,”Harmonics reduction with defected ground structure for a microstrip patch antenna,” Antennas and wireless Propagation letters, IEEE Transactions,2003.
7. K. Chang, R. York, P. Hall, and T. Itoh, “Active integrated antennas," Microwave Theory and Techniques, IEEE Transactions on, vol. 50, no. 3, pp. 937–944, Mar. 2002.
8. V. Radisic, Y. Qian, and T. Itoh, “Novel architectures for high efficiency amplifiers for wireless applications," Microwave Theory and Techniques, IEEE Transactions on, vol. 46, no. 11, pp. 1901–1909, Nov.1998.

DESIGN AND TESTING OF 512 BIT SRAM MEMORY CHIP WITH BUILT IN SELF-TEST USING XILINX/MODELSIM TOOL

Y. Kalavathi[1]., K.JAHNAVI[2]., K.Krishnapriya[3]., K.Pushpa[4]., K.Vasavi[5]

1 Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: vemireddy.kalavathi@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0450, 15RG1A0451, 15RG1A0452, 15RG1A0453), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— - In this work a memory chip with a size of 512 bits was designed using Xilinx or a model simulation software. The memory built in self-test (MBIST), or as some calls it, the in-matrix self-test, is an amazing piece of logic. Without a direct connection to the outside world, a very complex on-board memory can be tested efficiently, easily and inexpensively. This article describes the modeling and simulation of MBIST. The design architecture is written in VHDL (Very High Speed Integrated Circuit Hardware Description Language) code using Xilinx ISE tools. The verification of this architecture is done by testing the stuck SRAM for errors. A BIST algorithm such as March C and many others is implemented to test a failed SRAM.

Keywords— Built-in Self Test (BIST), Static Random Access Memory (SRAM), Integrated Circuit (IC), Dynamic Random Access Memory (DRAM), VHSIC Hardware Description Language (VHDL).

1. INTRODUCTION

Fast, low-power SRAMs are becoming a critical component of many VLSI chips. The speed of the processors and main memory is increasing, and the power dissipation is also increasing due to the increase in the speed of integration and operation and the increase in the number of devices being powered by the battery. SRAM helps bridge the gap and also reduces power dissipation. After designing the memory, let's move on to the memory failure test.

Following are the types of faults also called fault model:

- Stuck-at Fault
- State Transition fault
- Coupling Fault
- Addressing Fault and
- Data retention Fault

Stuck Failure - Abbreviated to SAF. This type of fault model assumes that a storage drive or a storage line is locked to logic "1" or logic "0".

State Transition Failure: This is part of the stuck bug where a memory reader or memory line cannot perform a 0-1 or 1-0 conversion after a write operation. These are referred to separately as high state transition faults and low state transition faults.

Docking station failed: Contains two drives. Changing the status of one drive changes the status of the other drive accordingly.

Addressing error: In this type of error model, a row or column decoder may not access the addressing unit, or multiple addresses are accessing the same storage unit at the same time, or an address is accessing multiple cells at the same time, or is accessing a different drive instead of the same specified drive .

Stuck Open Fault - With this type of fault model, a storage device is inaccessible. If the storage unit has only one input port, only a fixed output value is generated.

Data retention failure: With this type of failure model, a storage device cannot effectively keep its data value unchanged within the specified time period.

2. PROPSOED SYSTEM OF RAM ARCHITECTURE

The RAM BIST architecture is shown below. In the first block of the RAM-BIST architecture, the "ROM-based algorithm generator" was shown, in which the 8 algorithms are kept in an ideal state. This algorithm remains in an ideal state unless the BIST_EN signal is equal to "1" (or it is understood that the BIST operation will not start until the BIST_EN signal is equal to "1"). Among these 8 algorithms, one of the algorithms is selected based on the 8: 1 MUX selection line. Then the selected algorithm is transmitted to the "algorithm decoder". The read / write signal of this block is transferred to the built-in RAM to set the weather reading operation, or the write operation is carried out at the RAM address. The high / low signal is forwarded to the "address generator" to define whether a read / write operation is carried out in "addressing mode" or in "addressing mode down". This is decided by selecting the algorithm operation.

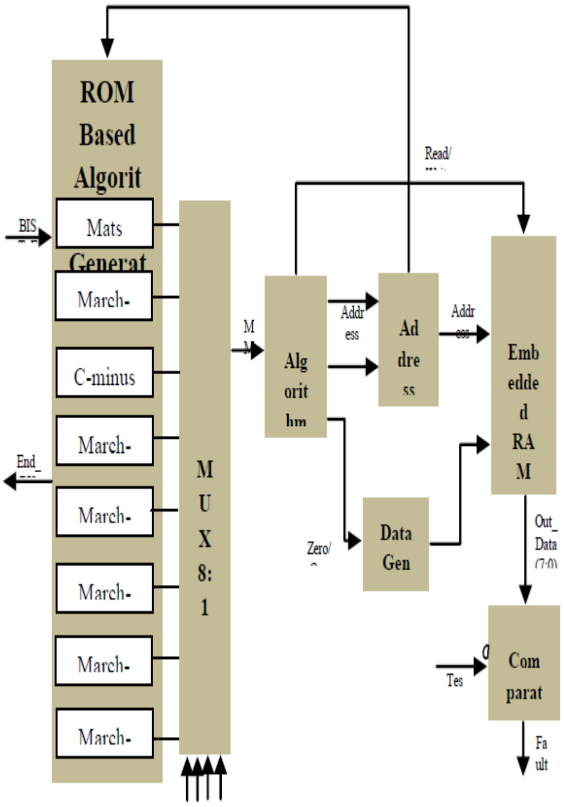


Fig. -1: RAM BIST architecture

Then the third zero / one signal is passed to the "data generator" to define that the read / write operation is being performed on bit "0" or bit "1". Therefore, depending on the state of the selected algorithm, the read / write operation is carried out in the RAM. Every time the "read operation" is carried out, data comes from the RAM and this data is transferred to the "comparator". In the comparator there is another input port (test data) at which the test input receives the same data as the data that was written into the "built-in RAM".

3. ALGORITHM FOR RAM TESTS

There are many types of test algorithms that are used for RAM testing. These algorithms are pretty straightforward for BIST implementations. The following table lists various test algorithms for RAM tests and the instructions that these algorithms execute of these entire test algorithms, the March-C algorithm comes in handy for providing the highest defect coverage. The error detection capabilities of March's test algorithms are summarized in the table below. All of these test algorithms are intended for RAM with one data bit per word, but multiple bits per word can also be used. In order to increase the error detection rate, a modification of the algorithm for sensitivity and coupling errors in the RAM is necessary.

Table -1: ALGORITHMS FOR RAM TESTS

No.	Algorithm	March Elements Code
000	MATS+	{↕(w0); ↑(r0,w1); ↓(r1,w0)}
001	March X	{↕(w0); ↑(r0,w1); ↓(r1,w0), ↕(r0)}
010	March C-	{↕(w0); ↑(r0,w1); ↓(r1,w0); ↕(r0,w1); ↓(r1,w0), ↕(r0)}
011	March A	{↕(w0); ↑(r0,w1,w0,w1); ↑(r1,w0,w1); ↓(r1,w0,w1,w0); ↓(r0,w1,w0)}
100	March B	{↕(w0); ↑(r0,w1,r1,w0,r0,w1); ↑(r1,w0,w1); ↓(r1,w0,w1,w0); ↓(r0,w1,w0)}
101	March U	{↕(w0); ↑(r0,w1,r1,w0); ↑(r0,w1); ↓(r1,w0,r0,w1); ↓(r1,w0)}
110	March LR	{↕(w0); ↓(r0,w1); ↑(r1,w0,r0,w1); ↑(r1,w0); ↑(r0,w1,r1,w0); ↑(r0)}
111	March SS	{↕(w0); ↑(r0,r0,w0,r0,w1); ↑(r1,r1,w1,r1,w0); ↓(r0,r0,w0,r0,w1); ↓(r1,r1,w1,r1,w0); ↕(r0)}

4. RESULTS OF THE SIMULATION

There are several types of tools that can be used as a simulator to perform the test phase of the design. This is done on the test bench. A test bench is a set of test stimulation times that match the circuit design. The response of the circuit under test can be read as waves. The reference file is responsible for providing input stimuli for the memory under test (MUT) such as a clock and various other test control signals. The response is then in the form of error signals, which are detected and displayed in the form of waveforms. In this project we used a model simulator. The result of the design is shown in the following section in the form of software screenshots. First, we show the screenshot of the RTL schema written in the Xilinx software.

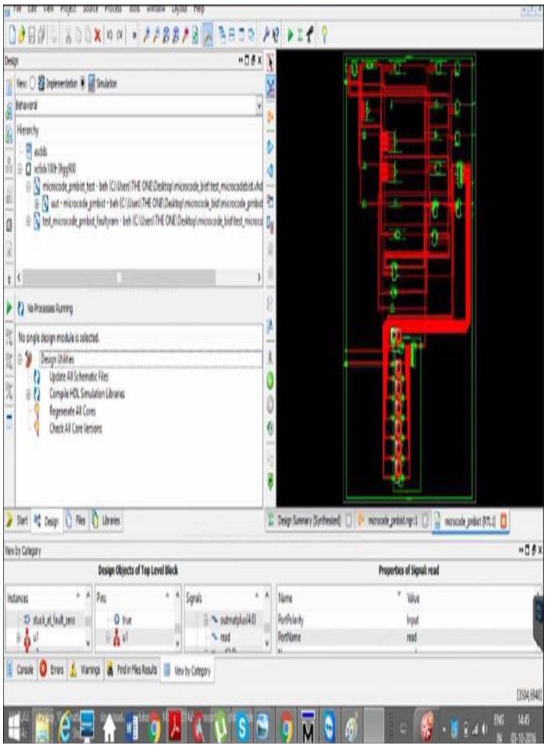
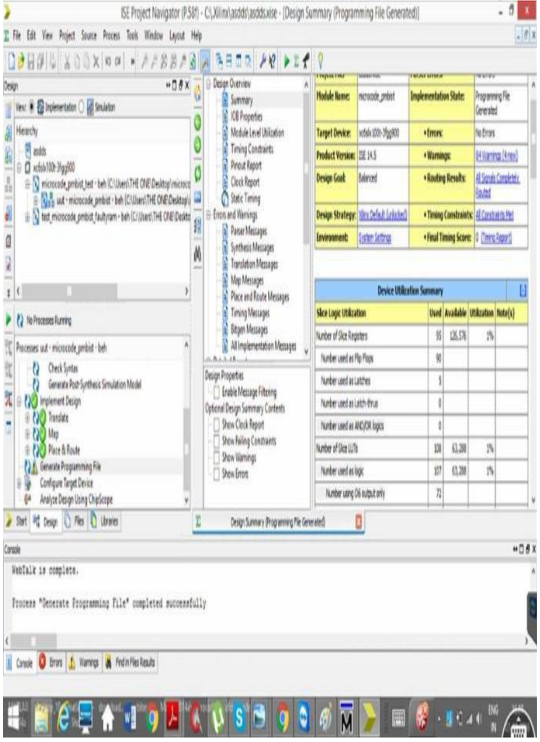


Fig. -2: RTL diagram in the Xilinx software

To do this, the software first asks you to select the elements. After we have selected the elements, we need to click on the Create Scheme tab. As soon as we click on this tab, we will see the RTL schema of the program.



```
WebTalk is complete.

Process "Generate Programming File" completed successfully
```

Fig. -3: Design summary in the Xilinx software

Then we simulate the VHDL code with the ISim simulator or the Modelsim software. Waveforms for all input and output parameters are displayed on the screen. So we can provide the input and monitor the output.

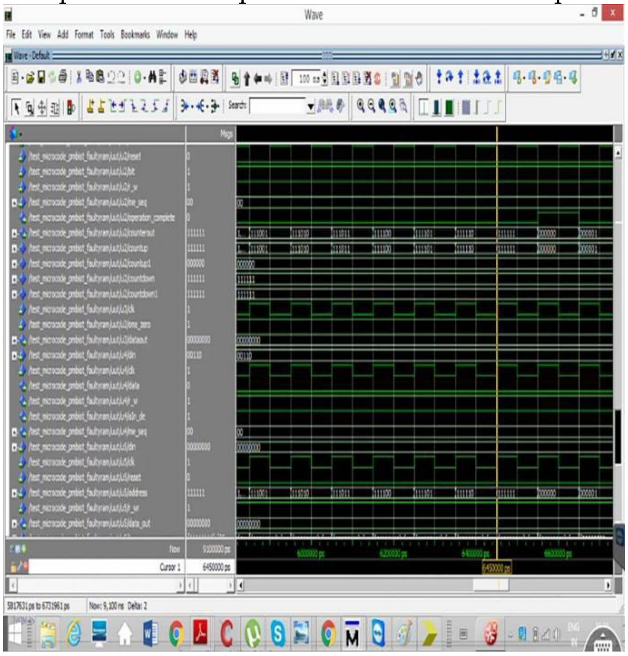
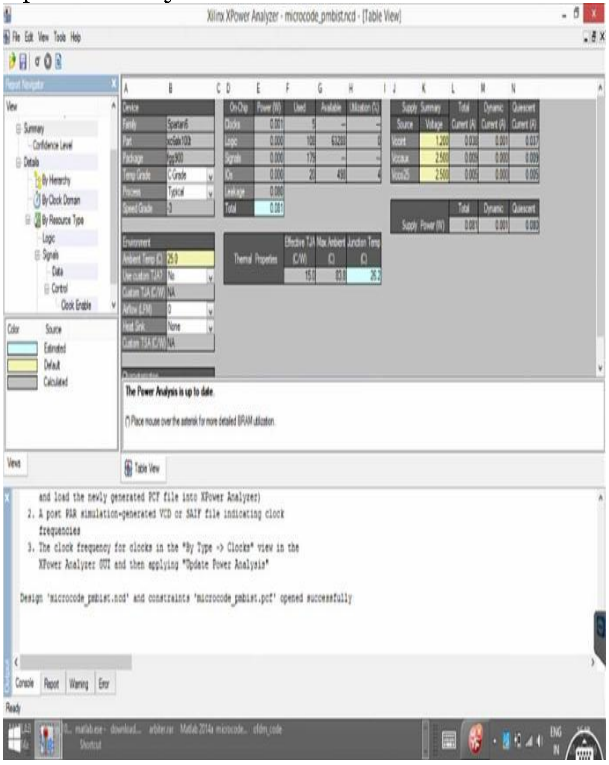


Fig. -4: Waveform in the Xilinx software

The following is the designed storage performance ratio as determined by the Xilinx Xpower analyzer.



The Power Analysis is up to date.

```
    and load the newly generated PCF file into XPower Analyzer)
  2. A post PAR simulation-generated VCD or SAIF file indicating clock
     frequencies
  3. The clock frequency for clocks in the "By Type -> Clocks" view in the
     XPower Analyzer GUI and then applying "Update Power Analysis"

Design 'microcode_pmbist.ncd' and constraints 'microcode_pmbist.pcf' opened successfully
```

Fig. -5: Performance analysis in the Xilinx software

5. CONCLUSION

This article describes the design of a 512-bit SRAM. We chose SRAM 6T as the storage bit cell and created an array designed with this bit cell in mind. We learned a lot about the low-power implementation of this SRAM 6T by looking at many documents such as how to make a SRAM 7T or SRAM 8T. The related work can be advanced to achieve a low power implementation. We understood many important concepts and learned tools that will help us in the future.

In short, a random access memory with built-in self-test has been successfully designed. BIST techniques are divided into online and offline tests. This project was developed at the entry level of VHDL so many changes can be made and additional architectures added to make the design more robust.

- The March-C algorithm can be used in design by simply changing the decoder in our project. This happens because the March C algorithm can cover the error better compared to other algorithms.
- We can increase the bit size to test more memory locations.
- BIST cannot insert the defective model. Therefore, in the future, we can work on

inserting a number of error models and then recognizing them.

• We can reduce the hardware coverage of the project by swapping the comparator and measuring device we use. This will improve the performance of our project.

• We can replace VHDL with Verilog HDL to reduce the command line for future work.

• Due to the unavailability of resources, we could not program this project on real FPGA hardware. Hence, future work can be done to run all of these tests through the FPGA hardware device and verify our work.

REFERENCES

1. Kalyana Srinivasa Rao, J Venkata Suman PG Student, Assistant Professor: Department of ECE, GMRIT, Rajam, Srikakulam, AP, “Low Power Design of A SRAM Cell for Embedded Memory”, International Journal of Research in Computer and Communication Technology, Vol 2, Issue 11, November- 2013.
2. Ad J. van de Goor, ComTex, Said Hamdioui, Halil Kukner, “Generic, Orthogonal and Low-cost March Element based Memory BIST”, Voorwillenseweg 201 2807 CA Gouda, The Netherlands and Delft University of Technology, Faculty of EE, Mathematics and CS, Mekelweg 4, 2628 CD Delft, The Netherlands.
3. Mária Fischerová, Martin Šimlaštík, “MemBIST Applet for Learning Principles of Memory Testing and Generating Memory BIST”, Institute of Informatics, Slovak Academy of Sciences.
4. Alberto Bosio, Luigi Dilillo, Patrick Girard, Arnaud Virazel, Leonardo B. Zordan, “An Effective BIST Architecture for Power-Gating Mechanisms in Low-Power SRAMs”, LIRMM, Montpellier, France.
5. Preeti S Bellerimath and R. M Banakar, “Implementation of 16X16 SRAM Memory Array using 180nm Technology”, International Journal of Current Engineering and Technology.
6. Xu Chuanpei, Tao Yi, Wan Chunting, “BIST method of SRAM for network-on-chip”, School of Electronic Engineering and Automatic, Guilin University of Electronic Technology, Guangxi Key Laboratory of Automatic Detecting Technology and Instruments, Guilin 541004, China.
7. M.H. Husin, S.Y. Leong, M.F.M. Sabri, R. Nordiana, “Built in self test for RAM Using VHDL”, Faculty of Engineering, Universiti Malaysia Sarawak 94300 Kota Samarahan, Sarawak.
8. Chih-Sheng Hou, Jin-Fu Li, and Ting-Jun Fu, “A BIST Scheme with the Ability of Diagnostic Data Compression for RAMs”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.

ANALYSIS OF THE SOIL QUALITY USING EXPERT SYSTEM FOR AGRICULTURE USING IMAGE PROCESSING TECHNIQUES

A. Anil Kumar[1]., P. Suresh [2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women.,

Maisammaguda., Medchal., TS, India (✉: anumula86@gmail.com)

2 Assistant Professor, Department of H & S., Anurag College of Engineering.,

Ghatkesar., Uppal., TS, India.

Abstract: Basically India is arable land. About 75% of Indians are farmers. However, some farmers still follow the traditional cultivation method. Traditional methods lead to inadequate and inefficient farming practices, as a result of which farmers do not receive the expected production and thus affect sales. However, by using an expert system, we can reduce the likelihood of these problems. Therefore, we examined the existing expert system for agriculture. And on this basis we will design an expert system for agriculture that consists of analysis of the soil to determine the quality of the soil and propose fertilizers based on the quality of the soil. Control plant diseases and grow the plants in a healthy environment. Keywords— Piezoelectric, Power generation, Vibration, Mechanical stress, Human body motion.

Keywords: sensors, image acquisition, segmentation, feature extraction, soil nutrients, explosion, brown spot

1 INTRODUCTION

In India, plant production has been drastically reduced. There are several factors that affect the overall return and decrease the overall profit. In India, farmers continue to use traditional methods to grow crops, control crop production, plant diseases that decrease crop production, and overall profit. To solve this problem and increase crop production, we will develop an expert system for agriculture. To do this, we examined various existing systems. With these existing systems in mind, we will design an expert system for agriculture using sensors and image processing techniques. The expert system uses sensors to get nutritional values from the soil and send them to the central processing system. The system processes this data, generates a result and displays information on soil quality. Another factor that the expert system will work on is plant disease. To determine the extent of the disease, the expert system uses image processing techniques including filtering, segmentation, feature extraction and classification. Based on historical data, the expert system will predict the extent of the disease and take preventive measures. In the case of plant diseases, we mainly focus on rice cultivation and on brown spots and epidemics. For this reason we will develop an expert system that will perform soil analysis and predict plant diseases.

Before you start formatting your work, first write and save the content in a separate text file. Keep your text and graphic files separate until the text has been formatted and designed. Don't use fixed tabs and limit the use of hard returns to a single return at the end of a paragraph. Don't add any kind of pagination on the paper. Don't number the headings, the template will do it for you.

Complete the editing and organizing of the content before formatting it. When checking your spelling and grammar, keep the following in mind:

2. LITERATURE SURVEY

Existing expert systems for agriculture are discussed in this section.

These expert systems have different aspects related to agriculture.

Here will be the general area of investigation

- Plant selection based on soil analysis report and market demand.
- Live weather updates on the internet
- Selection of pesticides and their amount according to symptoms and climatic conditions. [1]

2.1. Prediction of plant diseases

The identification of plant diseases is the key to avoiding yield and volume losses in agricultural products. This system helps in making decisions about plant diseases.

This software system is intended to support the decision-making of the technicians of the agricultural advisory service in the treatment of plant diseases. The system uses the Tropos methodology, an agent-oriented software development method that includes deliberate analysis techniques. The Tropos methodology is an agent-oriented software development methodology based on two key ideas, namely:

- Use of concepts at the knowledge level such as actor, goal, plan and stakeholder dependency during the entire software development process.
- The critical role assigned to the preliminary phase of needs assessment was to understand the environment in which the future system will operate.

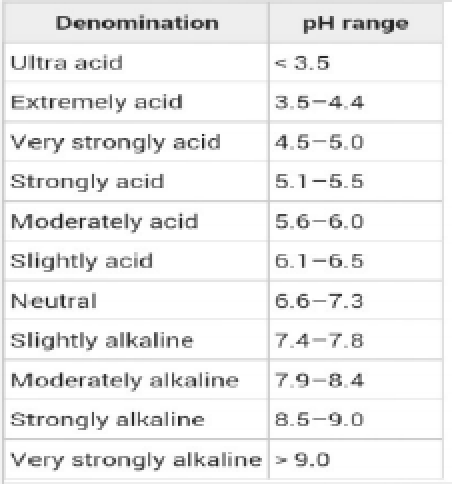
Topics covers four phases of software development:

1. Early needs analysis
2. Late needs analysis
3. Architectural design
4. Implementation

Other existing techniques for detecting rice diseases:

• Fractional zoom
• Artificial neural network

2.2. Soil Tests



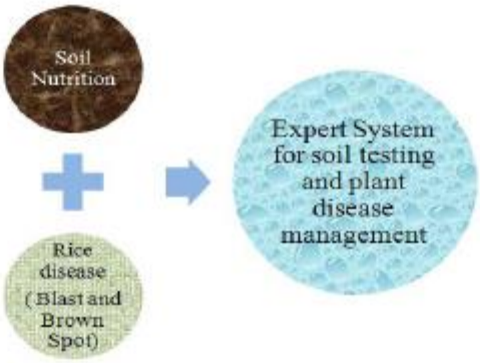
Denomination	pH range
Ultra acid	< 3.5
Extremely acid	3.5–4.4
Very strongly acid	4.5–5.0
Strongly acid	5.1–5.5
Moderately acid	5.6–6.0
Slightly acid	6.1–6.5
Neutral	6.6–7.3
Slightly alkaline	7.4–7.8
Moderately alkaline	7.9–8.4
Strongly alkaline	8.5–9.0
Very strongly alkaline	> 9.0

Table -1: Classification of the soil based on the pH value

This research takes into account the N, P, K, and pH levels of the soil to determine soil quality. It also offers harvests depending on the quality of the soil. Cultures can be selected based on pH values. The pH is nothing more than the percentage of hydrogen. It is the measure of acidity. The lower the pH, the higher the acidity. Acid cultures have a pH of 5 or less. Alkaline plants tend to have pH levels above 5-7. Fruits are acidic and have a low pH, while vegetables are alkaline and have a high pH. The following table shows the classification of the soil according to the pH value of the soil.

Smartphones have become a useful tool in agriculture because their mobility is the nature of agriculture, the cost of the device is very affordable, and the computing power allows a wide variety of practical applications to be created. In addition, smartphones are now equipped with various types of physical sensors, which makes them a promising tool for various agricultural tasks. This document systematically reviews the smartphone applications mentioned in the research literature that use sensors embedded in smartphones to provide agricultural solutions. [6, 7]

3. PROPOSED SYSTEM


Soil Nutrition
Expert System for soil testing and plant disease management
Rice disease (Blast and Brown Spot)

.

Fig. 1. Proposed system components

Based on the existing system, we will design an expert system for agriculture that takes into account two important factors for agricultural soil and plant diseases.

This system takes the input as the soil and the image of the plant using the sensor and the camera, respectively, and provides the information on soil nutrients and the disease level when the disease is the output brown spot and explosion. The following figure shows the process flow of the proposed system:

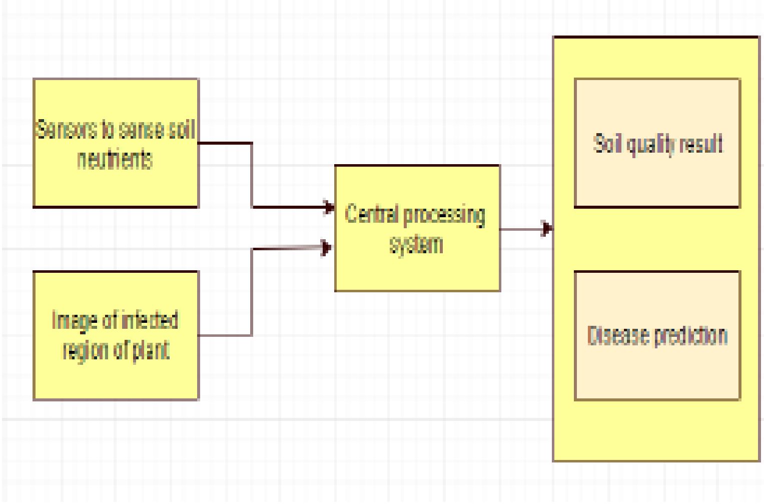

Sensors to sense soil neutrients
Image of infected region of plant
Central processing system
Soil quality result
Disease prediction

Fig. 2. Process flow of the proposed system

3.1 Description of the components:

1) First welcome form. When the user logs in to the system, a welcome screen is displayed that consists of two options: log in and log out.

2) If the user presses exit, the system will automatically shut down.
3) If the user presses Enter, the system will continue and the user can perform further operations.
4) The user should select options to obtain information about soil nutrients and predict plant diseases.
5) The system receives inputs from sensors and cameras and forwards them to central processing.
6) The central processor processes the input and the result is given to the user as output.

3.2 Technical data

A comparison with the available data is necessary to predict soil quality.
The existing system uses soil N, P, K and pH values to determine soil quality. However, in the system proposed with this main nutrient, we will take into account calcium, magnesium, sulfur and some trace elements (such as iron, manganese, copper) from the soil for better accuracy. [8th]
We have ideal nutritional value for the soil and we believe we will predict the quality of the soil. Here we also look at the weather. Depending on the soil quality and the climate, the system suggests a harvest for this soil.
This will help increase agricultural production with minimal losses. The second part of the expert system is the prediction of plant diseases. For this we consider two diseases, brown spot and rice rot.
These two diseases have different levels (stages). Using an image processing technology system, check the level and level of the screen, as well as the treatment and preventive changes for the disease.

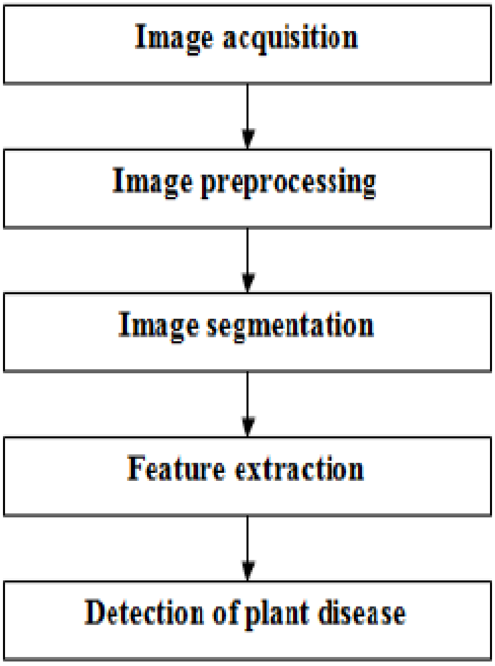
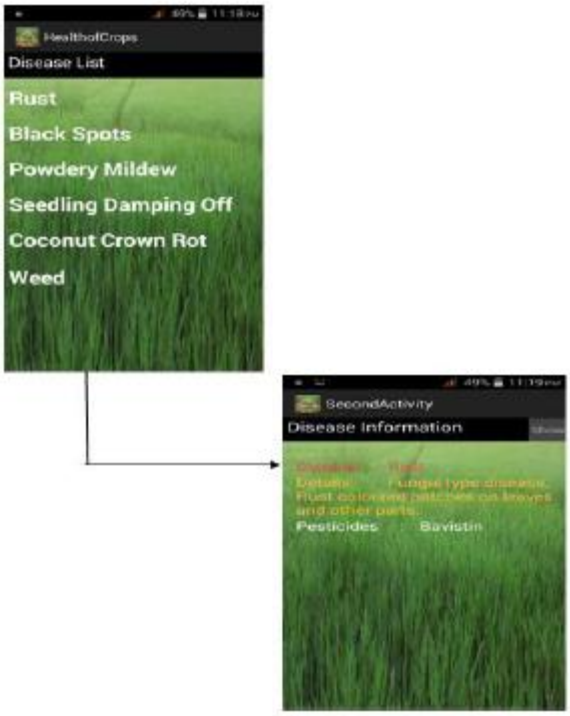


Fig. 3. Basic steps of image processing technology.

The third part of the expert system is the help option. Here the system provides useful information about agriculture, news related to agriculture, etc.



Disease : Rust
Details : Fungus type disease. Rust coloured patches on leaves and other parts.
Pesticides : Bavistin

Figure. 4. Module of the proposed system

The above illustration shows a module of the proposed system which is a "Help" button that provides information such as a list of diseases and information about those diseases.

4. CONCLUSION

This existing system will be analyzed on paper for agriculture and an expert system for agriculture will be proposed. The proposed system focuses on two factors: soil quality and plant diseases. This system will help increase overall agricultural production and minimize losses, which in turn will increase overall profits.

REFERENCES

1. Balmukund Maurya , prof. Dr.Mohd Rizwan Beg 2, Sudeep Mukherjee , “Expert System Design And Architecture for farming sector ” , IEEE Conference on Information and Communication Technologies 2013, pp 10 - pp 15
2. Anna Perini, Angelo Susi ITC-IRST, Via Sommarive 18, I-38050 Povo, Trento, Italy, ”Developing a decision support system for integrated production in agriculture ” , Environmental Modelling & Software 2003 ,pp 822 – pp 829
3. Santanu Phadikar,Jaya Sil,”Rice Disease Prediction Using Pattern Recognition Techniques ”,
4. International Conference on Computer and Information Technology, Dec 2008, pp 420 – pp 423
5. Y.Sanjana, AshwathSivasamy , SriJayanth ,”Plant Disease Detection Using Image Processing Techniques”, International Journal of Innovative Research in Science, Engineering and Technology May 2015 , pp 295 – pp 301

WEATHER FORECASTING SYSTEMS USING DATA MINING TECHNIQUES AND NUMERICAL PREDICTION MODELS

L.Prashanth[1]., D.Raj Kumar[2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉: prashanthlukkalpr@gmail.com)

2 Assistant Professor, Department of H & S., CMR Institute of Technology., Kandlakoya., *Medchal., TS, India*

Abstract: Data mining techniques have been the subject of several research articles. Climate change can have serious effects on the availability of human resources, especially in countries. The discovery of knowledge from temporal, spatial and spatiotemporal data is essential to climate change and the effects of climate on the environment. Climate change will have a significant impact on public health. Historical weather statistics for future forecasts. The development of the tools and techniques available to collect data on climate, water, temperature, etc. To prevent these public health effects, we can take action to prevent climate change by analyzing historical data. Climate change refers to long-term changes in weather conditions and patterns of extreme weather events. This can lead to changes in the threat to human health and multiply existing health problems. Go beyond empirical observations of the link between climate change and infection and develop a system that predicts the climate impact and what preventative measures should be taken by classifying and aggregating the data. Improvement of the prediction of spatio-temporal processes of climate change and the associated effects on different geographical scales.

Keywords: weather forecast, data mining and prediction algorithms, numerical prediction models over time.

1 INTRODUCTION

It is important to understand and improve the quality of the climate prediction system. Cool weather and environmental conditions are the flux of these, and the availability of hazards to humans, animals and nature can adversely affect humans. The river flow forecast therefore provides important information for the weather forecasting system. Global climate change challenges scientists and engineers to estimate and predict the full extent that Precision will download. Failures are defined as unfavorable situations with significant effects on the climate. Due to the unbalanced data volume, there is an error in the exact weather forecast. Data can be processed by combining data due to lack of data. The weather forecasting system is the application of science and technology to predict the atmosphere for a specific location or region. Weather forecasting uses data mining techniques to determine weather conditions. Most systems can depend on the weather forecast system. Predicting the weather was helpful in avoiding damage to life and much of the property. Weather forecasts such as temperature, humidity and precipitation, which are important in agriculture and other commodity markets. Let's take an example of a temperature forecast that many companies use to calculate or request a quote for the next few days. The forecast at that time can be used to plan activities and events, to plan ahead further and to survive. Many techniques are used today to weather forecast and improve forecast accuracy. There are different types of forecasts that are included in the weather forecast.

1.1. Background

In the field of weather forecasting systems, many researchers have tried to use certain data mining methods. K-means clustering involves dividing land and other areas to discover interesting patterns. Data set analyzed based on grouping and classification. The probability of the prediction is discussed over time. The time is predicted based on the uncertainties of the initial conditions and the formulation of the model. The accuracy of the results is more important because of the weather forecast as some people rely on location to handle their events. The reason depends on the weather in which the event decision is made. Work on the normalized data set in real time with the minimum-maximum normalization. Quantitative forecasts such as temperature, humidity and weather conditions are important in agriculture, for future planning and travel planning in the city, and for traders in commodity markets. Weather and climate disasters are increasing in India with no national capability to provide long-term weather forecasting. Many variables that can affect climate, given all current climate statistics and physical equations describing the interactions of particles at the smallest scale, are added to model a complete weather system. Assess the current state of science and determine what it takes to develop a long-term severe weather forecasting system for future forecasting and preventive action.

Foresight helps to take the necessary measures to largely avoid damage to life and property. Quantitative forecasts such as temperature and humidity are important both in agriculture and for traders in the raw material markets. The different categories of forecasting methods are: naive approach, assessment methods, quantitative and qualitative method, causal or econometric forecasting methods.

2. RELATED WORK

Yuko Tachibana and Mikihiko Ohnari present the model of hourly water consumption in a water treatment plant using a categorical approach, as the hourly water consumption must be predicted and the consumers must be supplied with water at the same time. The water consumption is represented as waves and is influenced by the time of the week and the temperature to which they are similar. The water consumption on public holidays and other days is not the same. By analyzing water consumption in large cities and applying data mining techniques, an accurate forecast for the year was made.

Andrew Kusiak and Shital Shah proposed a simple and effective alarm system to predict incoming water chemistry failures. This system is based on the modular system, is data-driven and based on data mining. In this system functions such as preprocessing, learning, prediction and display of the alarm generation. A decision making system for predicting water chemical faults with an alarm system. After the alarm, the boiler switches off.

Charles A. Doswell et al. Discuss the flood forecasting method. This is developed using the concept of ingredients. This is the result of heavy rains. It contains water vapor in the air and is also dependent on the precipitation of water.

Zhongnan Zhang et al. Describe the datagram association rule in large amounts of data to find important patterns so that the forecaster can predict extreme weather situations. An individual analysis is required for the weather analysis. Zhongnan Zhang et al. Proposed a new algorithm called DIAL to find some relationship between climate change and climate severity. The proposed algorithm consists of three steps: First, the static data set is changed, recording the weather conditions with the new data set by changing the climate trend for each measurement. Then apply the mapping rule to the newly generated dataset. Last predefined predictions for transferring the mediator rule into dynamic assignment rules between dimensions.

JP Evans tries to improve by introducing a regional climate model to characterize the river. Provision of information on the complex parameterization of the earth's surface in the regional climate model. Focuses on improving land modeling through climate feedback. Present a model to improve the predictive properties of the moisture deficit of water catchment areas - identification of unit hydrographs and component flows from precipitation, evaporation and runoff data (CMD-IHACRES).

PS Mohod et al. State that predicting precipitation and weather conditions is the world's most difficult problem in agriculture. Describes the data mining algorithms used for the determination. Neural Network (NN), Random Forest, Classification and Regression Tree (CRT), Support Vector Machine (SVM) and Nearest Neighbor K. These algorithms are used for prediction by default. Apply frequent extraction to the available data set to find common patterns. The data set often contains elements relating to parameters such as temperature, humidity and wind. These algorithms have been applied to the rainfall dataset for the past five years. Predict rain or not.

Priyanca Fargose, et al. Revised a better approach to weather forecast, studying the artificial neural network, ensemble neural network, backpropagation network, radial basis function network, general regression neural network, genetic algorithm, multilayer perceptron, fuzzy clustering, etc. for different types of weather forecast. The back-propagation algorithm is best for weather forecasting. The good neural network, which is automatic today, generates data itself and predicts weather conditions from the analysis of the data. The number of parameters can be taken into account to predict the time of day.

A. Makkeasorn et al. Have given a comparative study on the most important global climate changes between the neural network and the genetic algorithm. The study provides related details on sea surface temperature and location of precipitation using Next Generation Radar (NEXRAD). The study of artificial intelligence approaches comprises two parts of the neural network and the genetic algorithm. This work was assessed with the prediction of the correct climatic conditions by analyzing the SST and the metrological data.

G. Atsalakis and C. Minoudaki presented how water pumps can be planned and how one can try to minimize the costs involved. Studies consumer demand for water and predicts water distribution. The ANFIS technology (Neuro Adaptive Inferences -Fuzzy System) itself uses the prediction of the water distribution by removing the most recently saved details.

Ayham Omary et al. Examined weather and precipitation information using artificial intelligence and data mining techniques. The tool is used to save and analyze saved data. The analyzed data is fed to the AI engine and data mining in order to obtain further information about precipitation and future weather changes from the historical data.

3. PROPOSED SYSTEM

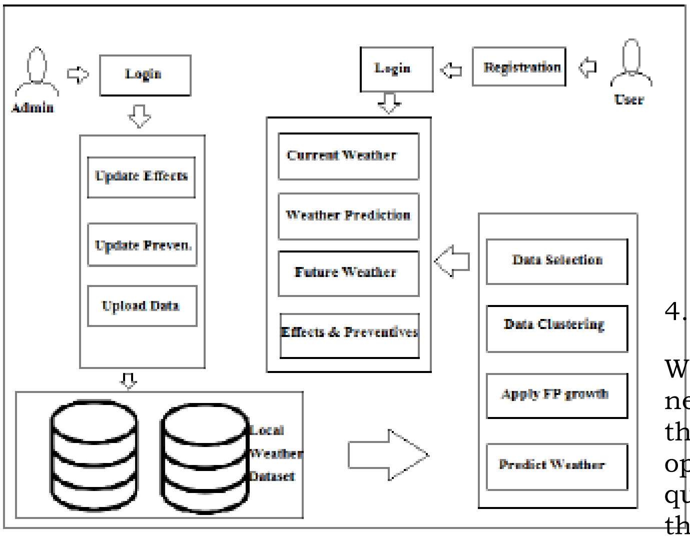


Figure 1: Proposed architecture

In this article we offer the weather forecasting system that predicts current and future weather conditions. Data mining techniques are applied to the dataset to extract useful information from the dataset. Such a grouping of data to find the frequent extraction of sets of elements and the genetic algorithm for the best adaptation of climatic conditions, impacts and preventive measures. The proposed system is shown in the previous figure. The role of the administrator is to upload data such as the impact of temperature and preventive measures and upload the record to the system. However, on the client side, the user has to register the application. As soon as the user has logged in, he receives the current temperature forecast and

Algorithm: FP-Growth FP-Growth reads transactions from both the data set and the mapping

1. A fixed order was used so routes can overlap when transactions share items. In this case the counters are incremented

2. Relationships between nodes that contain the same item are maintained, creating an individually linked list.

Algorithm 1: FP growth algorithm

- Future forecast with the effects of temperature and preventive measures. To predict the weather conditions in the proposed system, we use data mining algorithms. Share data and discover temperature or weather conditions. Grouping of the kmean and FP growth algorithms used.
- After this final input the temperature planned to find the most appropriate effects and preventive measures using the genetic algorithm.

4. RESULT

When collecting data, data is collected that is necessary for processing. We collected data in the city center and tracked each other from the open weather station for the region in question. They were compiled from data from the last few years. We took some parameters like temperature, wind humidity and weather conditions.

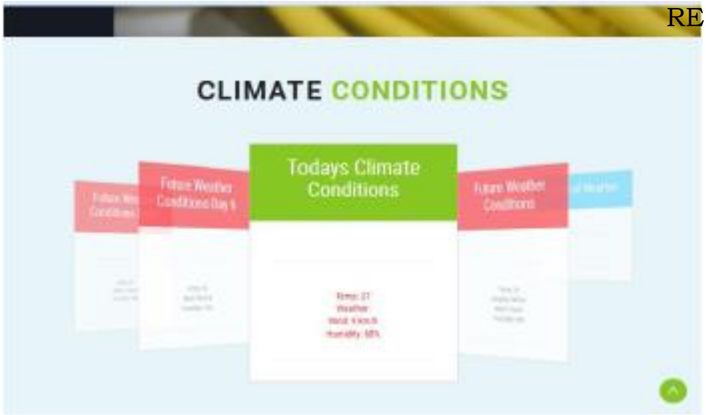

CLIMATE CONDITIONS
Future Weather Conditions Day 4
Todays Climate Conditions
Future Weather Conditions

Figure 2: Predicted weather with temperature

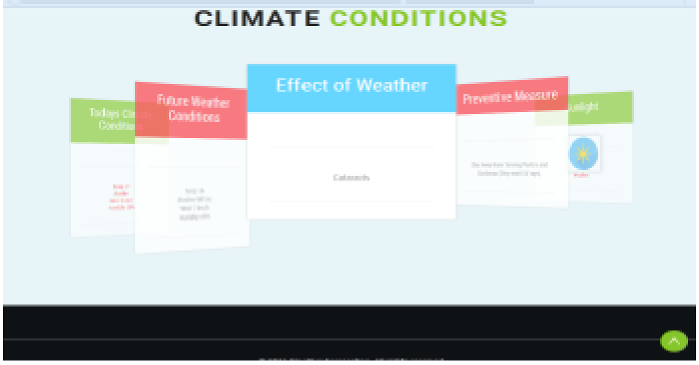
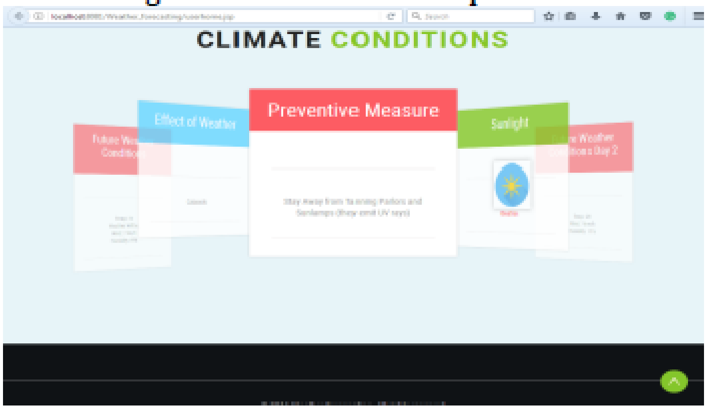


Figure 3: Effects of the temperature



Stay Away from Tanning Parlors and Sunlamps (they emit UV rays)

Figure 4: Preventives Measures

5. CONCLUSION

This system offers a first look at a project to create a numerical model for weather forecasting in the local climate. These models are generally complex and require a great deal of time and resources. Collect and have all the data you need and create a historical record of weather, precipitation and all possible associated attributes. It takes all the complex parameters as input and generates the smart models during the training and uses the same models to generate the predictions.

REFERENCES

1. Flash Flood Forecasting: An Ingredients-Based Methodology, Doswell, C. A., et al, 1996: Weather and Forecasting, 11 560-581
2. “Mining Dynamic Interdimension Association Rules for LocalscaleWeatherPrediction”, Zhongnan Zhang, Weili Wu, Yaochun Huang, Proceedings of the 28th Annual International Computer Software and Applications Conference (COMPSAC’04), 2004
3. Prediction Model of Hourly Water Consumption in Water Purification Plant through Categorical Approach, Yuko Tachibana and Mikihiko Ohnari, 1999. IEEE SMC '99 Conference Proceedings. 1999 IEEE International Conference on Systems, Man, and Cybernetics.
4. Data-Mining-Based System for Prediction of Water Chemistry Faults, Andrew Kusiak, and Shital Shah, IEEE Transactions on industrial electronics, vol. 53, no. 2, april 2006.
5. Improving the characteristics of streamflow modeled by regional climate models. Evans, J.P., 2003. J. Hydrology 284, 211 – 227
6. Amruta A. Taksande, P. S. Mohod Applications of Data Mining in Weather Forecasting Using Frequent Pattern Growth Algorithm

PREVENTING END-TO-END DELAY IN ZIGBEE BASED WIRELESS SENSOR NETWORK USING SHORTCUT TREE ROUTING

R.Mounika[1]., Y. Saritha Kumari[2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉: mounikarayaram001@gmail.com)

2 Assistant Professor, Department of H & S., Malla Reddy College of Engineering., Maisammaguda Medchal., TS, India.

Abstract: The Wireless Sensor Network (WSN) is the best solution for the rapid acquisition, processing and transmission of critical data. Sensor nodes can be used in a harsh environment, but the node batteries are low. Therefore, energy efficiency and network life are the main concerns of WSN. ZigBee has a low cost, low power consumption, and is useful in wireless sensor networks by choosing the appropriate communication protocol. Routing protocols such as AODV (On-Demand-Ad-Hoc-Distance-Vector-Routing), ZTR (ZigBee-Tree-Routing) and STR (Direct Access Tree-Routing) are compared in the basis for various performance metrics such as end-to-end delay, routing overhead, throughput, packet transmission rate (PDR). Mathematical analysis and performance evaluation show that STR performs better when compared to two other routing protocols.

Keywords: processors, receivers, senders, organization of computer systems, computer communication network, SMTP, ZTR, STR, protocol architecture (OSI model), protocol verification, routing protocols, distributed systems, client / server, distributed databases for databases.

1 INTRODUCTION

The basic idea behind this project is to find the most energy efficient routing protocol among the routing protocols. Since most wireless sensor networks use their own energy, i. H. Batteries, depleted, these WSNs establish a connection to different nodes of the networks and therefore use more energy by transferring the data in the nodes. To solve this problem, it is important to correctly select the route so that an optimal route is selected. We are therefore trying to find an energy-efficient routing protocol that reduces power consumption through efficient routing.

2. BRIEF REVIEW OF EXISTING TECHNIQUES

There are several routing management algorithms in the existing system, which are described below.

2.1 General routing techniques in the wireless sensor network

There are many routes for the delivery of data packets from the origin to the destination. Routing is the method of choosing the best route between them. Routing is done for many types of networks. However, we are mainly concerned with packet-switched networks. In this network, the packet is routed from the origin to the final destination via the intermediate nodes. The middle node refers to hardware devices such as routers, bridges, gateways, switches or firewalls, etc. During the routing process, packets are transmitted using the routing table, which keeps a record of routes to different networks.

Mobile Ad Hoc Networks (MANETs) have become an interesting and important technology in recent years due to the rapid proliferation of wireless devices. An ad hoc cellular network consists of mobile nodes that can move freely in an open environment. Nodes communicating in a mobile ad hoc network generally require the help of other intermediate nodes to establish communication channels. An ad hoc mobile network is a group of wireless mobile computers in which nodes work together by sending packets to each other so that they can communicate beyond the realm of direct wireless transmission.

MANET routing protocols can be divided into two categories:

- Proactive routing protocol
- Responsive routing protocol
- Hybrid routing protocol

2.2 Proactive Routing Protocol

Proactive routing protocols regularly update topology information and link changes throughout the network. You always have an up-to-date, optimal routing path. Proactive protocols retain routing information about routes available on the network even if those routes are not currently in use. The main disadvantage of these protocols is that maintaining unused routes can consume a significant portion of the available bandwidth if the network topology changes frequently. However, proactive protocols are not always suitable for highly mobile networks such as MANETs.

2.3 Reactive Routing Protocol

This protocol uses a deferred approach in which mobile nodes only discover routes to destinations when necessary. These protocols keep only the routes currently in use, reducing the burden on the network when only a few of the available routes are used at a time. Reactive protocols often use less bandwidth than proactive protocols, but the delay in determining a path can be significant. In reactive protocols, a route discovery process is usually required before packets can be exchanged between nodes because routes are only preserved while in use. This therefore causes a delay in the transmission of the first packet. Another disadvantage is that although route maintenance is limited to currently used routes, frequent changes to the network topology can still generate a significant amount of network traffic . Finally, packets transmitted to the destination can be lost if the route to the destination changes.

2.3 Hybrid Routing Protocol

The hybrid routing protocol combines proactive and reactive approaches to achieve a higher level of efficiency and scalability. However, even a combination of the two approaches must at least retain the network routes currently in use. Therefore, the number of topological changes that can be tolerated in a given period of time is limited. However, MANET differs from other networks through its highly dynamic topology. Numerous simulation results have shown that most topology-based routing protocols suffer from the highly dynamic nature of vehicle node mobility as they tend to have poor path convergence and poor communication performance. Location-based routing protocols have been identified as the most suitable routing protocols for MANET to achieve better performance and to demonstrate scalability and robustness in the face of frequent topological changes.

3. Proposed Routing Techniques

ZigBee routing is more efficient and includes different routing protocols. The reason for the design of the system is the comparative study of certain routing protocols and implement the most energy efficient routing protocol in ZigBee WSN.

3.1 Zigbee Routing Protocols

The protocols described above solve the routing congestion problem, but not the rerouting path problems and the traffic concentration problems. This is where the various routing protocols from ZigBee work.

They are:-

- ZigBee Tree Routing (ZTR)
- Direct access tree routing (STR)

3.1.1 Routing The Zigbee Wave

ZTR is designed to select the multi-hop routing path without the path detection method. In ZTR the addressing scheme for distributed blocks is used. In ZTR, each node is assigned a hierarchical address with the hierarchical addressing scheme, regardless of whether the destination is descending or ascending from the source or intermediate node.

The ZTR routing method is explained in Figure 1.

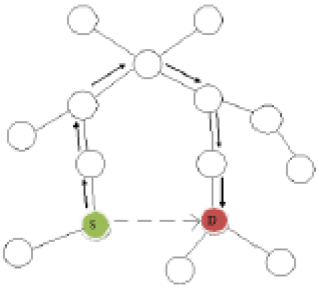


Fig. 1 ZigBee tree routing

The node, which can be a source node or an intermediate node, transmits the data packets to the primary node or to the secondary node by comparing its address with the destination address. In ZTR, each source or intermediate node sends data to the parent node when the destination is ascending and sends data to the child node when the destination is descending. Here, due to the routing topology of the tree, the packets are routed through several hops from source to destination, although they are in the range of 1 hop from source to destination. This problem is known as the redirect path problem. Another problem with ZTR is the problem of traffic concentration. In ZTR, all data packets pass through the same root node, which leads to an overload that leads to a collision of data packets.

3.1.2 Routing Of Direct Access Trees

The STR algorithm solves these two ZTR problems using the 1-hop neighborhood information. It completely solves the detour route problem, but partially solves the concentration of traffic. The STR algorithm essentially follows the ZTR, but selects one of the neighboring nodes as the next jump node if the remaining tree jumps can be reduced to the target. For example, in FIG. 4, STR calculates the remaining tree hops from the next hop to the destination for all neighboring nodes and selects N4 as the next hop to forward a packet to destination D2.

4. ARCHITECTURE OF THE PROPOSED SYSTEM

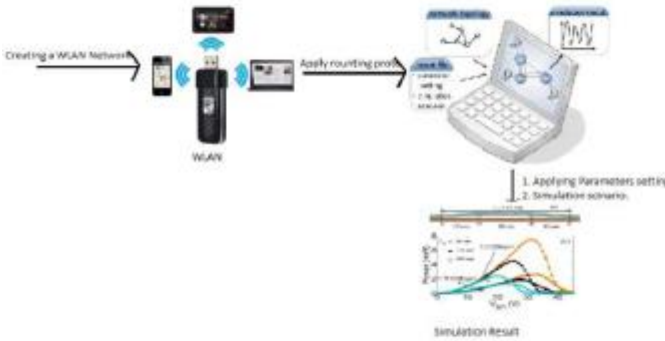


Fig 2: Architecture diagram

The main idea of STR is that we can calculate the remaining tree breaks from any source to a destination using the address hierarchy and the ZigBee tree as explained in the previous section. In other words, the remaining tree breaks can be calculated using the tree levels of the source node, the destination node, and their common ancestor node, since the packet of the source node goes back to the ancestor. Common, which contains an address of the destination, and goes to the destination in ZTR.

STR has the limitation that the routing path is not always optimal in one aspect of the end-to-end hop distance since the next hop node is selected based on local information such as the neighbor table at 1 hop.

For example, in Figure 4, the optimal path from S to D2 is S-N5-D2, but 2-hop neighborhood information is needed for source S to know that N5 is in D2's 1-hop communication area. . Obviously the maintenance of 2-hop neighborhood information creates a high protocol overhead in the network with a high node density. For this reason, we decided to provide a resource-efficient routing protocol from the standpoint of memory consumption and routing overhead.

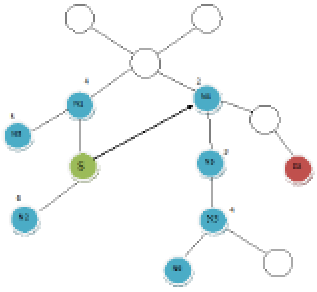


Fig.3: Routing the shortcut tree

5 ALGORITHM

```
Initialization
S = U —- where U is source node
For all nodes V
if V adjacent to U
D(V) = c(U,V)—– current cost of node for all node v adjacent u
else D(v) =
LOOP
Find w not in S with the smallest D(w)
Add W to S
Update D (v) for all V besides W and not for S.
D (v) = min D (v), D (w) + c (W, V) - continuous updating of D (v) when learning shorter paths
Until all nodes of S.
```

6 RESULT

The most energy efficient protocol.

- Agricultural fields

To measure moisture in the agricultural area and soil quality, STR can be efficient.

- Global temperature measurement technology

Routing protocols can be used to determine the temperature remotely.

- Detection of seismic waves from different positions

Prediction of seismic waves to avoid measurement losses.

- Detection of nodes

To find the energy efficiency protocol at the lowest cost, these techniques can be used.

7 CONCLUSION

In this system we overcome the problem of ZigBee routing protocols like AODV, ZTR. We suggest STR, which uses neighbor table based routing, originally developed for the ZigBee standard, and STR provides an efficient routing path H.

REFERENCES

1. Changjiang Li, Yufen Wang, Xiaojuan Guo “The Application Research of Wireless Sensor Network Based on ZigBee” 2010 Second International Conference on Multimedia and Information Technology
2. WANG Longkanga, NIE Baishenga, ZHANG Ruminga, ZHAI Shengruia, LI Hailonga “ZigBee-based positioning system for coal miners” First International Symposium on Mine Safety Science and Engineering Procedia Engineering 26 (2011) 2406 – 2414
3. Rashmi S. Deshpande, L. K. Wadhwa, “Overview of ZigBee based WSN” Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438
4. Mohammad Ali Moridi , Youhei Kawamura, Mostafa Sharifzadeh, Emmanuel Knox Chanda b, Hyongdoo Jang “based on radio waves attenuation using ZigBee”Tunnelling and Underground Space Technology 43(2014)362-369.

ROUTING AND PERFORMANCE ANALYSIS OF SCALABLE VEHICULAR AD HOC NETWORKS VANET

M.Uppa Mahesh[1]., V. Narasimha[2].,

1 Assistant Professor, Department of H & S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: maheshuppa18may@gmail.com)

2 Assistant Professor, Department of H & S., Swamy Ramanadatheerda Institute of Engineering and Technology., Nalgonda., TS, India.

Abstract: Routing in Vehicular Ad hoc Network is a tough job due to the same features of Mobile ad hoc network such as high mobility of nodes, dynamically alternating topology and highly subdivided networks. It is a challenge to confirm reliable, nonstop communication in the presence of fast moving vehicles. The performance of routing protocol depends on several internal factors mobility of nodes and external factors road topology and problems that block the signal. This demands an extremely adaptive approach to deal with the dynamic scenarios by selecting the best routing and forwarding strategies and by using appropriate mobility and propagation models. In this paper a comparison of different routing protocols like AODV, DYMO, OLSR and LAR1 with different scenarios using a scalable number of nodes is analysed and hence which protocol works better in urban area can be concluded.

Key Words: MANET, VANET, ITS, QualNet, AODV, OLSR, DYMO, LAR1.

1. INTRODUCTION

Vehicular ad hoc networks (VANETS) are different kind of mobile ad hoc networks (MANETs) that are formed between moving vehicles on required base. VANET are developing technology, which enables a wind range of applications, containing road safety, passenger convenience and intelligent transportation. The VANET helps to create safer roads by indicating the information about the road condition and traffic scenarios between the vehicles in a timely manner. Along with the safety applications, VANETs propagates valuable, real time information to the user such that transmitting information, weather information and other multimedia applications. VANETs takes some of the feature such that mobile nodes and self-organizing behavior from MANETs. However, VANETs have certain distinctive features such that high mobility of nodes, time changing density of the node, frequently changing topology, and these all makes them more challenging.

1.1 Issues Of Routing In Vanet

Even though VANETs are capable of allowing much different application, the design of operative intravehicular communication leftover as challenges. The node in the VANETs is designed by vehicles with high mobility. The node in VANETs can join any time and they can leave the network. The time changing vehicles density results in a quick change in topology, which make maintaining a route a tough job. This in turn, results in low throughput and high routing overhead and also affects the performance in VANETs producing less packet reception rate. The distribution from the high rise building makes problems such as routing loops and forwarding an incorrect direction, which gives more delay. The issue of passing network division and the issue of broadcast storm further complicate the design of routing protocols in VANETs.

2 DIFFERENT ROUTING PROTOCOLS

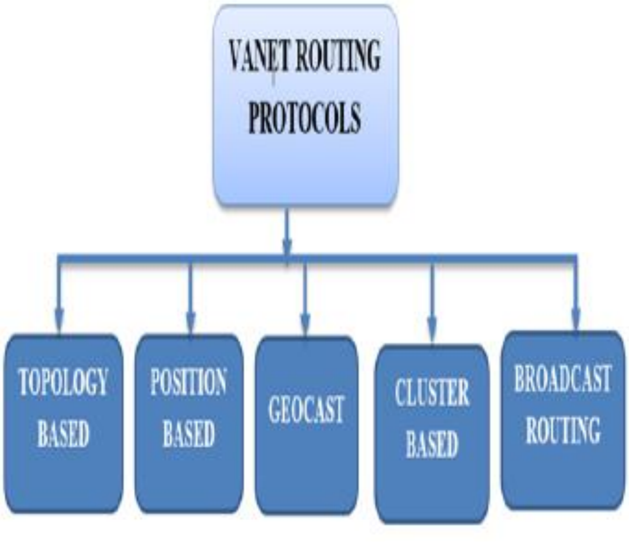


Figure 1:Routing protocols

Several routing protocols used in VANETs are topology based routing protocols, position based routing protocols, geo-cast based routing protocol, broadcast based routing protocols and cluster based routing protocols. These protocols are categorized according to their area of application. Figure 1 shows different routing protocols of VANETs.

2.1 AODV

The AODV is an on demand routing protocol. This protocol stores the routing table information between the nodes when it is required. It also collects the next hop router values for packets to forward. AODV has two parts first route discovery and second route maintenance.

2.2 OLSR

OLAR is a proactive routing protocol and also called as table driven protocol. In this protocol the routing table initially contents all the details of the nodes. Only symmetric links are used in OLSR for route setup development and relays. Every node in the network need to send its reorganized information to some selective nodes called as Multi Point Relays (MPR), which resends this information to its other selective nodes. The nodes which are not in MPR set can read and process the packet. MPRs are also used in route calculation to form the route from source to destination node.

2.3 DYMO

The DYMO is a Dynamic MANET On demand. It is a reactive routing protocol. The DYMO is a less memory stores routing information and provides control packets when a node receives the packet from route way. The initial process of DYMO source router to provide a route request (RREQ) message to destination routers. Intermediate node store route information added to routing table.

2.4 LAR1

Location aided routing, is an improvement to flooding algorithms to decrease overhead. Most on demand approaches, containing DSR and AODV use flooding to find a route to the destination. LAR1 goals to decrease the overhead to send the route request only into a defined area, which is probably to have the destination. This results in an adjustment between decreased overhead and increased latency which wants to be balanced correctly.

3. PROPOSED SYSTEM

The performance of different routing protocols like AODV, OLSR, DYMO and LAR1 are simulated for VANET scenarios using QUALNET Simulator. Here considered the simulation area of 3000mx3000m, with bidirectional road as a background image in a scenario. Here considered different number of nodes in a scenario to analysis the various parameters like total packet received, throughput, delay and jitter with all routing protocol. The simulation study focused on packet delivery ratio, throughput, Delay and jitter. The simulation parameters for the network scenario are described in Table below.

Simulator	QUALNET
Terrain size (m)	3000*3000
Urban Terrain format	QualNet format
No. of Terrain Files	1
Data type	CBR
Radio/Physical Layer	802.11p CCH and 802.11p SCH
Pathloss model	Urban model Autoselect
Propagation Environment	Urban
No. of channels	2
Channel frequencies	5.92GHz and 5.95GHz
Antenna Model	Omni Directional
Routing Protocols	AODV,OLSR,DYMO,LAR1
No. of Nodes (Density)	10,25,30,50,60
Simulator time(sec)	580,560,600,600,550

Table 1: Simulation Parameters

The different number of nodes scenario like 10, 25, 30, 50 and 60 nodes scenario setup are constructed and the sample scenarios of 10 and 60 nodes are shown in figures below figures 2 and figure 3 respectively. The scenario setup consists of all device, link and wireless subnet connections. The mobility connections between the vehicular nodes and with the road side units are established in scenario setup.

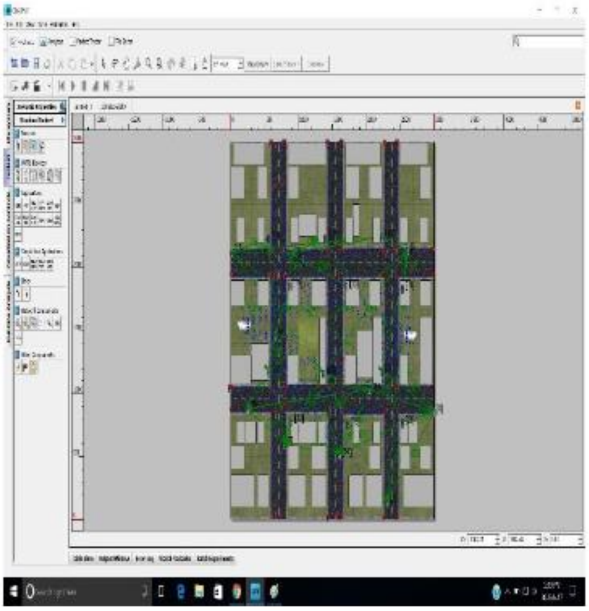


Figure 2: 10 Nodes scenario

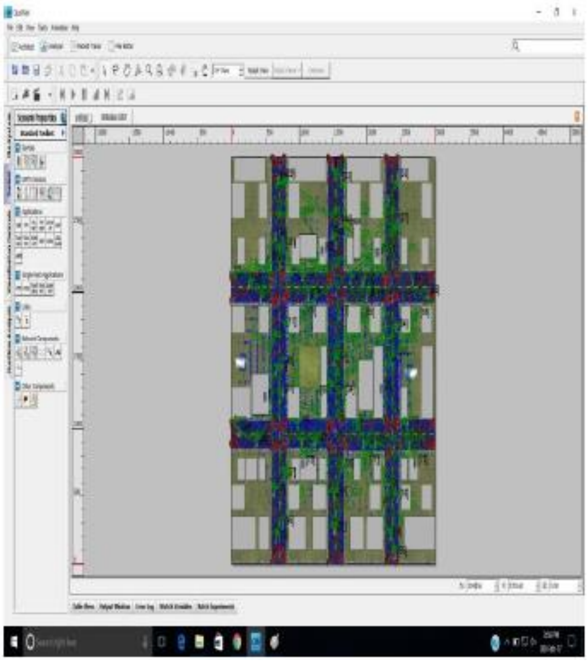


Figure 3: 60 Nodes scenario

6. RESULT ANALYSIS

The four parameters considered for analyzing are Total Packet received, Throughput, End to end delay and jitter. This parameter was analyzed for different routing protocol AODV, OLSR, DYMO and LAR1 for different scalable node scenarios. The comparison is shown in the graphs below.

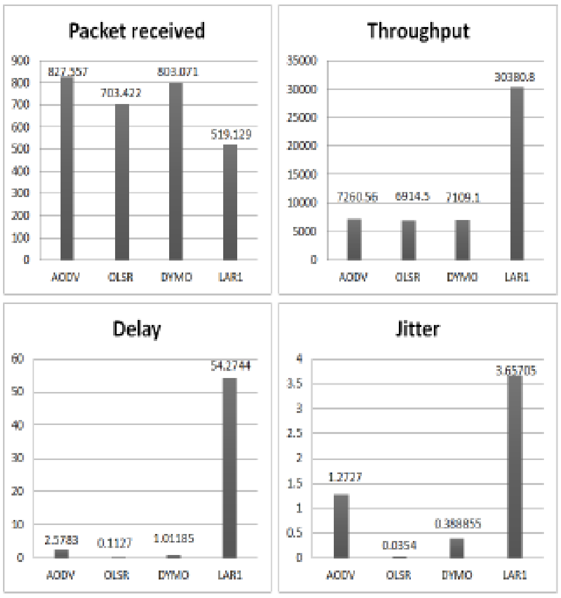


Figure 4: 10 Nodes Scenario

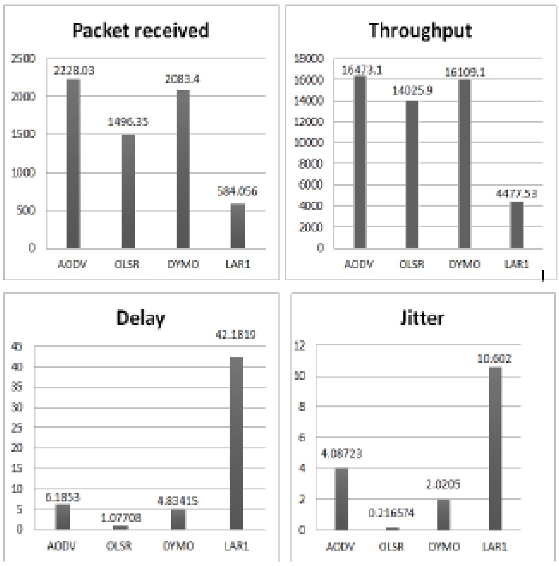


Figure 5: 25 Nodes Scenario

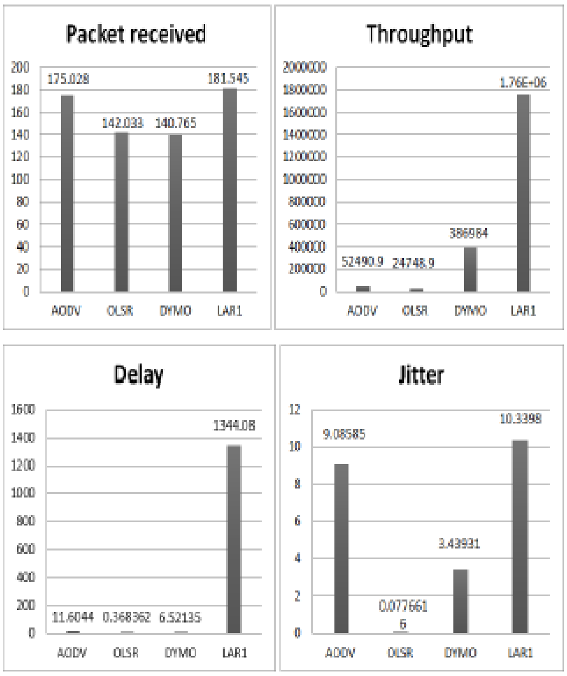


Figure 6 : 30 Nodes Scenario

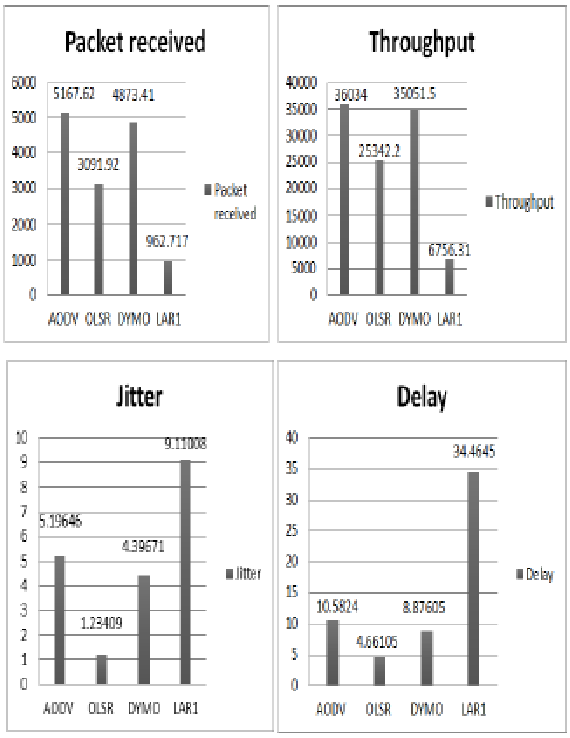


Figure 7: 50 Nodes Scenario

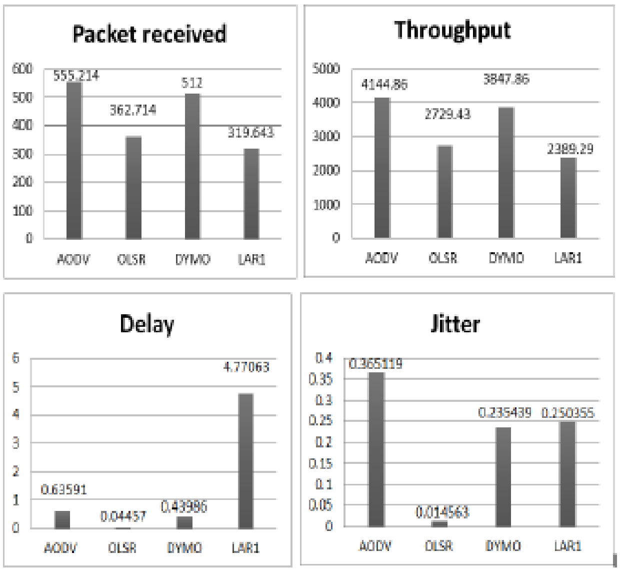


Figure 8 : 60 Nodes Scenario

7. CONCLUSION

From the above results, it may be concluded that the packet received in all node scenarios for AODV routing protocol gives better result. The LAR1 routing protocol gives more throughput and delay, whereas OLSR and DYMO routing protocol gives average parameter values for all scenarios compared to AODV and LAR1 routing protocols, hence by the above analysis, consideration for the best protocol with respected to parameters considered, for an actual scenario can be selected.

REFERENCES

1. Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).
2. Zeadally, Sherali, Ray Hunt et al. ", Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50, no- 4 pp- 217-241, Springer, 2012.
3. F. Li and W. Yu, "Routing in Vehicular Ad Hoc Networks: A Survey," Vehicular Technology Magazine, IEEE, vol. 2, no. 2, pp. 12–22, 2007.
4. YaseerToor et al., "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, 3rd quarter, vol 10, No 3,pp. 74-88, 2008
5. VANET Parameters and Applications: A Review Kamini Rakesh Kumar Vol. 10 Issue 7 Ver. 1.0 September 2010 Global Journal of Computer Science and Technology.
6. K. C. Lee, U. Lee, and M. Gerla, "Survey of Routing Proto-cols in Vehicular Ad Hoc Networks," in Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, M. Watfa. IGI Global, 2010, ch. 8, pp. 149–170.
7. R. Kumar and M. Dave, "A comparative study of various routing protocols in vanet," CoRR, vol. abs/1108.2094, 2011.

SECURE STORAGE AND MANAGEMENT OF DATA IN CLOUD COMPUTING USING SHA ALGORITHM

A.Anil Kumar[1]., L. Prashanth[2].,

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: anumula86@gmail.com)

2 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉: prashanthlukkalpr@gmail.com)

Abstract: The main idea of this document is to ensure the integrity of the cloud storage area. To ensure security in cloud computing, we use the SHA algorithm. With this method, some important security services, including key generation, encryption, and decryption, are provided in the cloud computing system. Here, the TPA is the trusted entity that has the experience and skills to assess the security of cloud storage on behalf of an on-demand data owner. The main purpose is to securely store and manage data so that only authorized users can access it.Keywords— Pulsed latch, Shift register, Flip-flop, CNTFET memory devices.

Keywords: SLA, AES, DES, HTTPS

1 INTRODUCTION

Cloud computing is seen as an important part of a business to meet demand at low cost. It is internet-based computing in which the application, platform and infrastructure are provided as a service. The main concept of this technology is that customers only pay for the services they use. Resources can be geographically assigned anywhere and provide the type of service the user wants. Now the user no longer needs to have physical infrastructure. Instead of storing the information on your individual hard drive or requests to be notified of your requirements, you can install them elsewhere over the Internet to collect your information or use your requests. This can increase the persuasive evidence of confidentiality. This information technology is the distribution of facilities over the network. Cloud installations allow individuals and businesses to customize the software and hardware that other people make in remote locations. Cloud computing instances include web document storage, community interaction websites, webmail, and online business services. This archetype of computer technology enables computers and information servers to be used from any location where a network connection is available. This computing technology provides a common set of servers that includes information storage space, networks, computing power, and specific business and consumer needs.

2 CLOUD COMPUTING CAPABILITIES

Here are the characteristics of cloud computing that explain its relationship and how it differs from traditional computing:

- Virtualization: Virtualization refers to the abstraction of computing resources (CPU, memory, network, storage, application stack and database) from the applications and end users who use the service. This is a technique that allows hardware resources to be multiplexed and users to run multiple operating systems on the same physical hardware. This technology enables a single data center or high-performance server to be split up so that they function as multiple machines. The number of virtual machines a system can partition depends on the system's hardware configuration.
- On-demand self-service: Consumers can provision or remove services at any time without the need for human contact with the service provider. Whether software, platform or infrastructure - everything is offered as a service in the network.
- Elasticity: With elasticity, the user can purchase more resources for a short time if necessary and pay for the required capacity or capacity. When these resources are no longer needed, the user can return this function.
- Location independence: Allows users to access systems through a web browser regardless of their location or the device they are using (PC or mobile phone). The services are made available to users all over the world using their smartphones, laptops, tablets and

desktops. These devices can be used anywhere with a simple online access point.

- Multi-Lease : Cloud providers serve several companies with the same infrastructure and software. This approach is more energy efficient than installing multiple copies of software on different infrastructures.
- Autonomous: To provide highly reliable services, clouds behave autonomously by managing themselves in the event of a failure or degradation.
- Metered Services: Due to the affordable nature of the cloud, the user can pay with a pay-as-you-go model. The cloud provider can measure the storage and processing tiers, the bandwidth and the number of user accounts that can be billed accordingly.
- Maintenance: Cloud computing is easier to maintain because it doesn't need to be installed on each user's computer and is accessible from multiple locations.

3 CLOUD COMPUTING CHALLENGES

- Security and data protection: This includes the backup of stored data and the monitoring of cloud usage by service providers. This challenge can be solved by storing data internally and using it in the cloud. Therefore, the security mechanisms between organizations and the cloud must be robust.
- Service delivery and billing: Service level agreements (SLAs) with providers are insufficient to ensure availability and scalability, as the dynamics of the services make it difficult to assess the associated costs.
- Interoperability and portability: Since the cloud environment is very dynamic for user requirements and due to the concept of virtualization, the leverage effect of migration to and from resources and applications should be allowed. In addition, change providers should switch between clouds as required and there should be no blocking times.
- Reliability and availability - cloud providers always lack 24-hour service, which leads to frequent outages. Therefore, it is important to monitor the service provided by internal or third-party tools.
- Automated service delivery: A key characteristic of cloud computing is elasticity. Resources can be assigned or released automatically. Therefore, a strategy is needed to use or free up cloud resources, maintain the same performance as traditional systems, and use optimal resources.
- Performance and bandwidth costs: Organizations can save money on hardware but have to spend more on bandwidth. This can be inexpensive for smaller applications, but significant for data-intensive applications.
- Virtual machine migration: With virtualization technology, an entire machine can be viewed as one file or a series of files. To unload a heavily used physical machine, you must move a virtual machine between physical machines. The main goal is to distribute the load in a data center or collection of data centers.
- Energy costs: The cloud infrastructure consumes large amounts of electrical energy, which leads to high operating costs and carbon dioxide emissions.

4. PROPOSED WORK

The aim of the work is to examine the security constraints and to focus on the current dangers of the actual security practices for fashionable cloud computing for cloud computing systems. His determination has helped scientists evaluate security arrangements at different stages to differentiate fears in the many cloud computing prototypes that have been modeled by internal and external customers. Hence it will be beneficial.

Explain the cloud security protocols that protect the cloud environment.

Although cloud computing is widespread, research into managing resources in the cloud environment is still in its infancy. The main aim of the research work is to examine the improved and efficient approaches to the use of resources that are relevant for the cloud-based system. Here is a brief description of the work to be done:

- A system will be developed to maintain the integrity of the information exchange between the participating systems.
- A scheme is developed to authenticate the participating system involved in the communication.
- A system will be developed to guarantee the confidentiality of the information exchanged between the participating systems.
- A safe model is developed that includes the previously developed diagrams.

Similar to full IT diagrams, cloud computing organizations essentially uncover security problems early on, that is, the application phases and project phases of their upgrade process. It solves the principle in a system that is more robust, safer and more error-free than systems that classify safety substances only once after processing the system. Because of the difficulty of the cloud environment, the actual advancement of a cloud computing scheme requires a review of these security vulnerabilities and a requirement for common approaches to be identified earlier in the expansion process. This invites you to mirror the entire cloud. In cloud computing environments, internal fears have gradually improved from previous ages. For the people, the inner danger represents the fears that are controlled within the association. Internal customers with a connotation usually have additional information from the data reserved there in and in the future, which is better informed about how this information and requirements should be billed than external customers. While internal fears cannot be completely separated, real barriers can be developed to break them down.

4.1 Symbolization and initiations

- FEncod: This is a script document that contains the encoded information and the document is kept in CSP3.
- FTemp: It is determined by the information processing period (recovery process and drive must be free) and is a preliminary document.
- Gen_Key (): This creates a protected key.
- Ks - This is a key generated by the Gen_Key procedure in CSP-2.
- Encoding (): This is the encoding method used to encrypt the document.
- Decoding (): This is a decoding method for decrypting a document.

This procedure negotiates with many additional rules. The clients interact through the gateway server using the HTTPS procedure to download their information. The Docker Docker Swarm repository clustering procedure enforces the top disposition on the gateway server. Thus, the document sent by the client is transported directly to a node of the swarm collection, where the swarm monitor carries a display to enter a repository and the information unit is organized and the repository opens the SSL procedure to encode the information via AES, RSA or a typical additional encryption methodIn certain circumstances, the client focuses on transmitting its information, sets up a call over HTTPS on the gateway server, at which point the gateway server retrieves the document from the storage server and forwards it to its node for decoding, the a procedure contains similar to coding. The decoded information is pulled through the gateway server and can then be retrieved by the client for retrieval.

Our proposed arrangement has two important helpers:

1) Efficiency and Security: - The strategy proposed by Security is to depend on reserved and unrestricted encryption of the keys. This is clear and efficient in the practice of undisclosed key generation and hashing. Therefore, the restrictions of each interval occur and the key exchange takes place in a safer place than with the symmetric and asymmetric procedure. However, our strategy is more efficient than the other methods as it does not require a lot of information to be coded when subcontracting, or additional support in the presentation part, and the portion is protected in a complementary way as we code the information to do this avoid illegal third parties. Vacation. Distinguish your subjects.

2) Open Verifiability: Our strategy is one key difference in offering free authentication. Authorization: The person who receives information about the server in addition to the owner has checked their competence as they do not need the information for the coding of individual fragments.

5. ANALYSIS OF THE RESULTS

Implementation is the development phase where the guesswork becomes a functional method. This can therefore lead to the phase of maximum uncertainty still existing in order to achieve a new effective system and to give the customer the certainty that the new system requires effort and remains operational. The operational phase includes preparing suspects, examining the current system and its limits of execution, agreeing on approaches to achieving an exchange, and evaluating exchange approaches.

Here our goal is to measure the encryption and decryption speed of each algorithm for different packet sizes. The performance of the encryption scheme is calculated by dividing all of the plaintext in encrypted megabytes over the total encryption time of each algorithm. The power consumption of this encryption technology decreases as the performance value increases. Taking into account the different sizes of data blocks (0.5 MB to 20 MB), the algorithms were evaluated with regard to the time required to encrypt and decrypt the data block. All implementations were correct to ensure that the results were relatively fair and accurate.

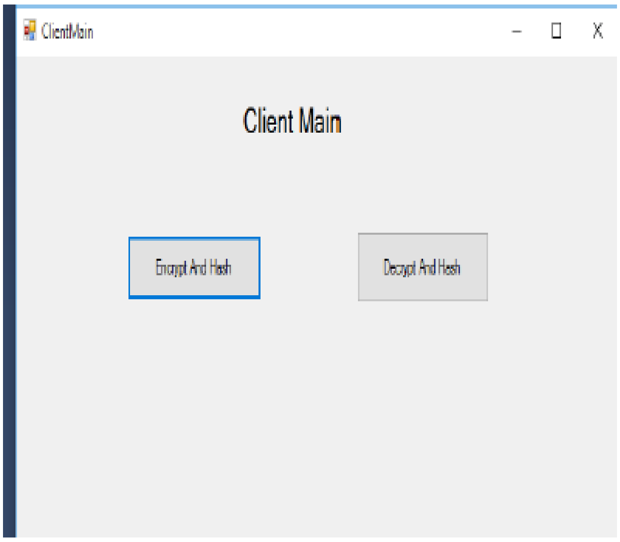


Figure 1: First open the .NET. Encryption and hash for encryption purposes.

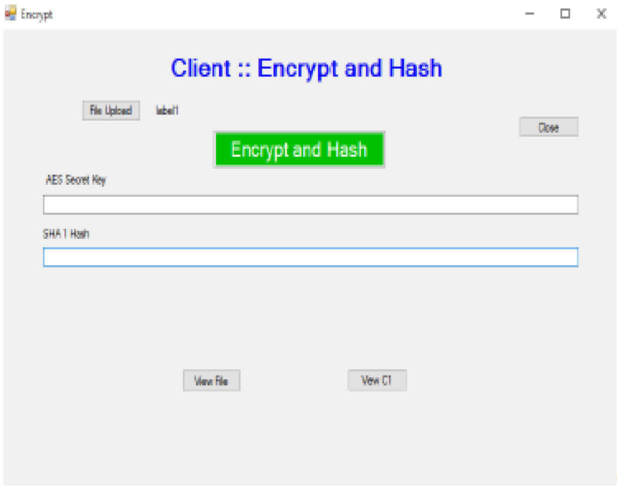
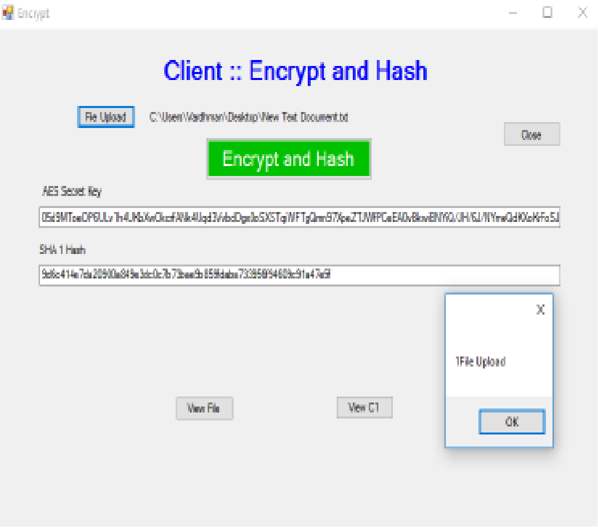


Figure 2: File successfully uploaded" after uploading of file.



C:\Users\Vardhman\Desktop\New Text Document.txt

AES Secret Key

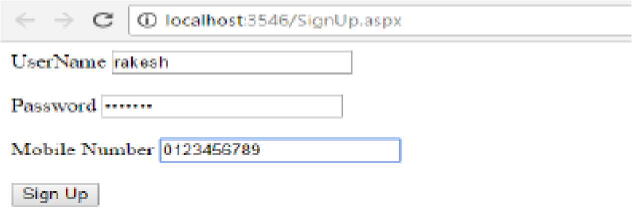
05d9MTcaDP8ULv Th4UMbXwOkcfANk4Uqd3VvbdDgx0sSXSTqWFTgQmn97kpaZTWPCaEA0vBkwBNYQ/JH/6J/WYnwQdK0oKfs5J

SHA 1 Hash

9d6c414e7da20900a849e3dc0c7b73bae9b859bdaba73395894609c91a47a9f

1File Upload

Figure 3: encrypted file of that uploaded file



localhost:3546/SignUp.aspx

UserName rakesh

Password •••••••

Mobile Number 0123456789

Figure 4: Fields username, email id and mobile number of the user which are used earlier

Now we need to choose the file to download by clicking the Choose File button. Then click on Download file button.

6. CONCLUSION

In this proposal we have given an overview of the security of information storage in cloud computing and projected a framework based on an encryption system. To ensure the security of customer information stored in the cloud, we are planning an efficient and operational encryption approach to improve the security of data at rest. We have shown that our agreement almost guarantees the security of information when it is held in the information center of a cloud service provider (CSP). This will help create an ideal for information protection in cloud computing. This architecture is capable of immeasurably expanding customer compliance and will attract many nominees in this area for both developed and future research farms.

REFERENCES

I. Brandic, “Towards self-manageable cloud services”, IEEE International Conference on Computer Software and Applications, pp. 128-133, 2009.

M. Alhamad, T. Dillon and E. Chang, “A survey on SLA and performance measurement in cloud computing”, On the Move to Meaningful Internet Systems: OTM 2011, Springer Berlin Heidelberg, pp. 469-477, 2011.

Aderemi A. Atayero, Oluwaseyi Feyisetan,“Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption”, In Journal of Emerging Trends in Computing and Information Sciences, Vol-2, No.10, pp.546-552, October 2011

In 32nd International Conference on Distributed Computing System Workshops, pp.573-577, 2012 (2012) W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.t. Abdullaha, “Cloud-Based Intrusion Detection Service Framework”.

A REVIEW PAPER OF REMOVING OF FLUORIDE IN WATER

V Janaki[1]., K Amitha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- vjanaki7@gmail.com)

2.Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:-kamithatha123@gmail.com:-)

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract- Water is the main component of human survival. The main sources of water are rivers, lakes, ponds, reservoirs and surface runoff. Three quarters of the earth's surface is covered with water. In order to preserve the fragile ecosystem, the physico-chemical parameters of waters play a very important role. These parameters are changed due to the entry of pollutants into bodies of water. Among the water pollutants, fluoride also causes significant contamination of drinking water due to natural and anthropogenic activities that pose a serious threat to humans and humans. Animal health. Hence, it is necessary to remove fluoride from drinking water. This article describes a study of methods for removing fluoride from water such as coagulation and precipitation, reverse osmosis, nanofiltration, electrodialysis, ion exchange, electrocoagulation, and adsorption.Keywords: Resin, Antioxidant, Gallic Acid, Extraction, Adsorption, Separation.

Keywords: Fluoride, Precipitation, Ion-exchange, Adsorption, electrocoagulation.

1 INTRODUCTION

Water is the most important component as it is the basic medium for the origin of life [1]. The chemical composition of water depends primarily on its uses for domestic, industrial, and agricultural purposes. 0.6% of the total water resources are covered with groundwater, which can be consumed in both rural and urban areas of India. Nowadays, the groundwater is polluted by urbanization and industrialization. The main pollutants are hydrocarbons, heavy metals such as nickel, fluorides, nitrates, etc. that affect human health. Fluoride as a contaminant in groundwater causes a major problem in the supply of drinking water. It exists as inorganic fluorides or organic fluorinated compounds [2]. Depending on the fluoride concentration in drinking water, it is beneficial or harmful to health [2, 3]. Fluoride is beneficial for bone and tooth mineralization, fertility maintenance, hematopoiesis, and activation of enzymes such as adenylate cyclase [4]. It is a known fact that less

The uptake of fluoride reduces the susceptibility to tooth decay in humans [5]. A few decades ago, the use of fluoridated toothpaste to prevent dental caries was an obsession, but it was soon obsolete due to increasing reports of adverse effects on oral health, such as the occurrence of perioral dermatitis [6]. According to the WHO, the maximum permissible fluoride concentration is 1.5 mg / l [7]. The permissible limit for fluoride in Indian drinking water is 1 mg / l [8].

2. SOURCES

Fluorite, apatite and phosphate rocks as well as igneous and sedimentary topaz rocks are the most common naturally occurring fluorine-containing minerals and a source of fluoride in drinking water [9]. Milk is generally responsible for exposure to low levels of fluoride. Fluoride is consumed due to the ingestion of tea, which is reported in a range of 0.04 mg to 2.7 mg per person per day [10]. The presence of alkaline soil near water sources contaminated with fluoride is a prominent feature of areas affected by fluoride [11]. The main sources of fluoride can be divided into two categories:

1) Natural sources:

- Herbs and feed grains
- The water
- Volcanic activities

2) Anthropogenic Sources

- Mixture of minerals and other nutritional supplements
- Fluoride in the air
- Industrial wastewater
- Agrochemicals and household products

3. HEALTH EFFECTS

Several researchers had investigated that in the past 5 to 6 years, the influence and accumulation of fluorides throughout life caused damage to the human skeleton and teeth, as well as changes in DNA structure, paralysis of the will, cancer, etc. [12]. Susheela reported on the effects of fluoride pollution on human health, such as joint pain, viz. Neck, back, hips, shoulders, and knees with no visible signs of accumulation; nonulcerative dyspepsia, viz. Nausea, vomiting, stomach pain, flatulence / gas formation in the stomach, constipation, followed by diarrhea, etc. [13]. Czarnowski et al. He explained that increasing fluoride intake affects human bone density, urine and hair. [14].

3.1 HUMAN HEALTH

3.1.1 Tooth fluorosis:

In dental fluorosis, the enamel loses its shine due to the high fluoride absorption during permanent dentition and mainly affects children. The mild form of dental fluorosis is recognized by chalk-white teeth, while the yellowish-brown pigmentation in the center of the teeth and severe pitting of the teeth occur. The effects of dental fluorosis may not be noticeable if the teeth are fully developed prior to overexposure to fluoride. Just because an adult shows no signs of dental fluorosis doesn't necessarily mean their fluoride intake is within safe limits.

3.1.2 Skeletal fluorosis:

Skeletal fluorosis affects both children and adults. It does not manifest itself until the disease reaches an advanced stage. In the early stages of skeletal fluorosis, patients complain of symptoms of arthritis. Fluoride builds up in the joints of the shoulder, neck, pelvis, and knees, making it difficult to move, walk, and bend. In later stages, skeletal fluorosis is characterized by restricted movement of the spine and is therefore easy to diagnose. The advanced stage is osteoporosis.

3.1.3 Non-skeletal fluorosis / other problems:

In addition to skeletal and dental fluorosis, excessive fluoride intake can lead to degeneration of muscle fibers, low hemoglobin levels, red blood cells (red blood cells) deformities, excessive thirst, headaches, rashes, nervousness, and neurological manifestations (affecting brain tissue) similarly like in people with Alzheimer's disease pathological changes), depression, gastrointestinal problems, urinary tract problems, nausea, abdominal pain, tingling in fingers and toes, decreased immunity, repeated miscarriages or stillbirths, male infertility, etc. Changes in the functional mechanisms of the liver, kidneys , Digestive system, respiratory system and excretory system.

3.2 ANIMAL HEALTH:

Almost all land and aquatic animals are sensitive to high doses of fluoride, although tolerance varies from species to species. For terrestrial animals, drinking water, soil, or vegetation are major sources of excessive fluoride intake, which naturally contain excess soluble fluorinated compounds or are contaminated with fluorinated compounds released by volcanic eruptions or industrial activities.

3.2.1 Invertebrates:

Many invertebrates are very sensitive to fluoride toxicity. Bees and silkworm larvae are very sensitive to fluoride toxicity. The silk industry in several countries has been severely affected by industrial fluoride contamination [16, 17]. Aquatic invertebrates and vertebrates, including fish, are also sensitive to fluoride toxicity. In general, freshwater or freshwater aquatic animals have a lower fluoride tolerance than marine or hard-water animals [18].

3.2.2 Vertebrates:

In terrestrial vertebrates, herbivores are more sensitive than carnivores and other animals that rank higher in the food pyramid. Domestic and wild herbivores are more exposed to environmental pollutants because they cannot selectively eat and consume contaminated food, feed and water.

It is therefore necessary to bring the fluoride concentration to the required level. Here are some overviews of articles on the different techniques available to remove fluoride from water.

4. METHODS FOR DEFLUORIDATION OF WATER

Sl.no	Removal Method	Process	Advantages	Disadvantages	Name of the Author	Medium used	Reference numbers
1	Coagulation and Precipitation	Involves the addition of chemicals and the formation of fluoride precipitates	1. Commonly used 2. It is more practical. 3. Easy to understand	1. Low treatment efficiency upto 70% 2.Requirement of large dosage of chemicals for treatment. 3.Requirement of skilled manpower	Meenakshi et.al., Lawler,D.F. et.al., Larsen,M.J. et.al., Qafas,Z.et.al., Dahi,E et.al., Aldaco et.al.	Aluminium sulfate and lime (NEERI METHOD),salts of Calcium, aluminium and iron, bone char combined with sodium dihydrogen phosphate and calcium chloride, granular calcite.	20-25
2	Reverse Osmosis	It is a physical process in which the anions are removed by applying pressure on the feed water to direct it through the semi permeable membrane.	1.Membrane can be completely recovered after every arrangement of examination. 2.This can remove 90% of fluoride regardless of initial concentration	1.Non attainable for rural regions. 2. Very expensive. 3.Skilled labor required. 4.Need pH improvement.	Ndiaye et.al. Behanu et.al Gedam et.al. Diawara et.al.	1. RO membrane of Ethiopian Rift Region, 2.Polyamide RO Membrane, 3.Low Pressure RO	26-29
3	Nano Filtration	It removes the larger dissolved solids when compared with RO.	1. High productivity. 2. No Chemicals needed. 3.used for wide range of pH.	1. Highly expensive technique. 2. Prone to fouling, scaling or membrane degradation.	Tahaikt et.al. Pontie et.al. Bejaoui et.al.	1.NF90 2.NF400.	30-32
4	Electro-coagulation	Technique for applying direct current to sacrificial electrodes that are submerged in an aqueous solution.	1.obliges basic equipment 2.simple to handle 3.less support cost 4.treated water is consumable, colorless and odourless	1.electrodes should be consistently supplanted 2.utilizes high electricity 3. Loss of productivity due to the formation of oxide film on the cathode.	Yang et.al. Feng Shen et.al. Drouiche et.al. Un et al. Bennajah et al.	Aluminium electrodes, Iron cylindrical reactor as anode,	44-47
5	Adsorption	Adsorption is the bond of molecules species from bulk solution for a surface of a solid by physical or chemical forces.	1. Ease of operation. 2.Adsorption procedure in worthwhile 3. High productivity for fluoride removal and can remove up to 90% fluoride. 4. Cost effective. 5. Produce high quality water. 6. Regeneration is conceivable.	1. Process is dependent on pH. 2. Regeneration is required. 3. Disposal of fluoride-laden material.	Kariyanna et.al. J.P. Barbier et.al., Muthukumaran et.al., Rongshu et.al., Y.Min et.al., Y. Wang et.al., Nava et.al., Padmavathy et.al. Theragaonkar et.al. Gandhi et.al. Mohapatra et.al. Amit Bhatnagar et.al. Prins Satish et.al.	Activated alumina, activated carbon coated with silica gel, calcite, activated saw dust, activated coconut shell powder, activated fly ash, groundnut shell, coffee husk, rice husk, magnesia, serpentine, bone charcoal, orange peel, chalk powder	48-60

4. CONCLUSION

A variety of factors and geological conditions directly or indirectly influence the correlations between different pairs of physicochemical parameters of water samples. Some parameters are measured directly by their respective measuring devices, others are determined by titrimetric methods, and some elements like fluoride need to be treated with different methods. Since it is necessary to treat the fluoride present in the water, this poses many problems. The fluoride treatment method can be chosen based on the advantages and disadvantages among which adsorption is the best method for removing fluoride from water according to the study.

REFERENCES:

1. Muturu C., Onyango,M.S. et.al. – 'Fluoride removal performance of Phosphoric acid treated lime: breakthrough analysis and point-of-use system performance. Water SA,38 (2),279-286.
2. Kirck KL (1991) Biochemistry of the elemental halogens and inorganic halides. Plenum, New York; pp 19-68.
3. Treasure ET, Dever JG (1992) The prevalence of caries in 5 year old children living in fluorinated and non

fluorinated communities in New Zealand NZ Dent J 88:9-13.

4. Mellete JR, Aeling JL, Nuss DD (1983) Perioral dermatitis J Assoc Military Dermatol 9:3-8.
5. WHO (World Health Organisation), 2006, Guidelines for Drinking Water Quality: Incorporating First Addendum toThird Edition. World Health Organisation, Geneva., 375 p.
6. Misra, A.K. and Mishra, A., 2007, Study of quaternary aquifiers in Ganga Plain India: Focus on groundwater salinity, fluoride and fluorosis. J. Hazardous Mater., 144, 438-448.
7. Teotia, S.P.S., Teotia, M. and Singh R.K., 1981, Hydro-geochemical aspects of endemic skeletal fluorosis in India- An epidemiologic study., Fluoride, 14 (2), 69-74.
8. Czarnowski, W., Krechniak, J., Urbanska, B., Stolarska, K., Taraszewska-Czarnowska, M. and Muraskzo-Klaude, A., 1999, The Impact of Waterborne Fluoride on Bone density, Fluoride, 32 (2), 91-95.
9. Payel Roy, Ritesh Kumar and Goutham Kumar Roy, Fluoride Pollution Abatement, Research gate.
10. Bourbon P (1967) Analytical problems posed by pollution by fluorine compounds J Air Pollut Control Assoc 17:661-663.
11. Weinstein LH, Davison A (2004) Fluorides in the environment: effects of plants and animals. CABI Publishing, Cambridge.
12. Surendra Roy, Gurucharan Dass, 2013, Fluoride Contamination in Drinking water, Resources and Environment, 3(3), 53-58.

FINDING A UTILITY THRESHOLD FOR ACCURATE ITEMSET DIGGING

Dr. P Geetha[1]., K Amitha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- pgeetha123@gmail.com)

2.Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:-kamithatha123@gmail.com:-)

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

ABSTRACT: Within this paper, we address all the challenges by proposing a singular framework to find the best-k high utility itemset mining, where k may be the preferred quantity of HUIs to become found. High utility itemsets (HUIs) mining is definitely an emerging subject in data mining, which describes finding all itemsets getting a software application meeting a person-specified minimum utility threshold min-util. However, setting min-util appropriately is really a difficult problem for users. Two kinds of efficient algorithms named TKU and TKO are suggested for mining such itemsets with no need to set min-util. We offer a structural comparison of these two algorithms with discussions on their own advantages and limitations. Empirical evaluations on real and artificial datasets reveal that the performance from the suggested algorithms is near to those of the perfect situation of condition-of-the-art utility mining algorithms. The present studies may succeed in certain applications, they aren't produced for top-k high utility itemset mining but still are afflicted by the subtle problem of setting appropriate thresholds. We propose a method known as NU that is applied during the making of the UP-Tree. Utilizing a parameter k rather from the min_util threshold is extremely desirable for a lot of applications. The TKU formula adopts a concise tree-based structure named UP-Tree to keep the data of transactions and utilities of itemsets. TKU inherits helpful qualities in the TWU model and includes two phases.

Keywords: Top-k pattern mining, top-k high utility itemset mining, Utility mining, high utility itemset mining.

INTRODUCTION

Pomegranate belongs to Punicaceae family. Punica granatum (Punicaceae), commonly called pomegranate, recently described as nature's power fruit, is a plant used in folkloric medicine for the treatment of various diseases. The Pomegranate has strong antioxidant and anti-inflammatory properties, recent studies have demonstrated its anti-cancer activity in several human cancers. In addition, pomegranate peel extract with an abundance of gallic acid flavonoids and tannins has been shown to have a high antioxidant activity. Antimicrobial drug resistance in human bacterial pathogens is a worldwide issue and as a consequence, effective treatment and control of such organisms remain an important challenge. The chemical formula is C6H2(OH)3COOH. Gallic acid is found both free and as part of tannins. Salts and esters of gallic acid are termed 'gallates'. Despite its name, it does not contain gallium. Gallic acid is commonly used in the pharmaceutical industry. Gallic acid can also be used as a starting material

in the synthesis of the psychedelic alkaloid mescaline .Gallic acid seems to have anti-fungal and anti-viral properties. Gallic acid acts as an antioxidant and helps to protect human cells against oxidative damage. Gallic acid was found to show cytotoxicity against cancer cells, without harming healthy cells. Gallic acid is used as a remote astringent in cases of internal haemorrhage. Gallic acid is also used to treat albuminuria and diabetes. Gujar et al 2010 [1] has extensively studied extraction of catachin and epicatechin from Indian green tea leaves. The detailed study of effect of various operating parameters has been studied in the current work. The effect of microwave irradiation on thymol extraction shows increase in the percentage extraction of thymol from ajowain seed [2]. This present work deals with extraction and purification Gallic acid from peel of pomegranate to use it to biological and chemical test as standard compound by resin adsorption.

2. EXTRACTION OF GALLIC ACID

Materials & Methods

Instruments: Lab equipment was provided by Aavanira Biotech Private Limited, absorbance measurements was made on Thermo UV/Visible spectrophotometer with a pair of matched quartz cells of 1 cm width, Elder digital balance used for weighing.

Materials: All Raw materials purchased from local Market Pune. All the chemicals and reagents were of analytical grade and were purchased from Gandhi chemicals and Bioresource life science.

Selection of Common Solvent: After assessing the solubility of polyphenol in different solvents Ethanol has been selected as common solvent for developing spectral characteristics.

Soxhlet Extraction

Soxhlet extraction is a procedure for extracting nonvolatile and semi volatile organic compounds from solids such as dry powder, peel, soils, sludge's, and wastes. The Soxhlet extraction process ensures intimate contact of the sample matrix with the extraction solvent.

Preparation of Pomegranate Peel Extract

10 gm of pomegranate peel was used with 500 ml of ethanol and kept in an extraction thimble. The extraction thimble drained freely for the duration of the extraction period with the condenser attached to the top of the soxhlet apparatus. Soxhlet extraction was conducted for about 8 hours and the crude extract was used as a raw material for adsorption. The maximum amount of gallic acid is 0.35 mg/10 gm of peel of pomegranate.

Pretreatment of Adsorbent

10 gm of anion exchange resin Amberlite IR 400 was weighed and taken in a 250 ml conical flask. The adsorbent was washed with distilled water, then with 15 times w/v 0.5 (N) HCl and 0.5 (N) NaOH, and finally again with distilled water till neutral pH was obtained.

Batch & Continues Adsorption Study

10 g of pretreated resin suspended in buffer was kept in a 250 ml of conical flask. 50 ml of pomegranate peel extract (in 50% aqueous-ethanolic solution) with known polyphenol concentration was added to each flask. The flasks were kept in a shaking incubator maintained at 120 rpm and 25°C until adsorption equilibrium was reached. The temperature range was varied from 25-40°C, and pH of the buffer solution was varied from 4-7. The buffer pH of 4-5.5 were obtained using citrate buffer (an equimolar (0.1 M) mixture of citric acid and tri-sodium citrate). For pH 6-6.5, phosphate buffer (an equimolar (0.2 M) mixture of sodium dihydrogen phosphate and di-sodium hydrogen phosphate) were used. The adsorptive capacity of the resin is represented by the following expression. [3]

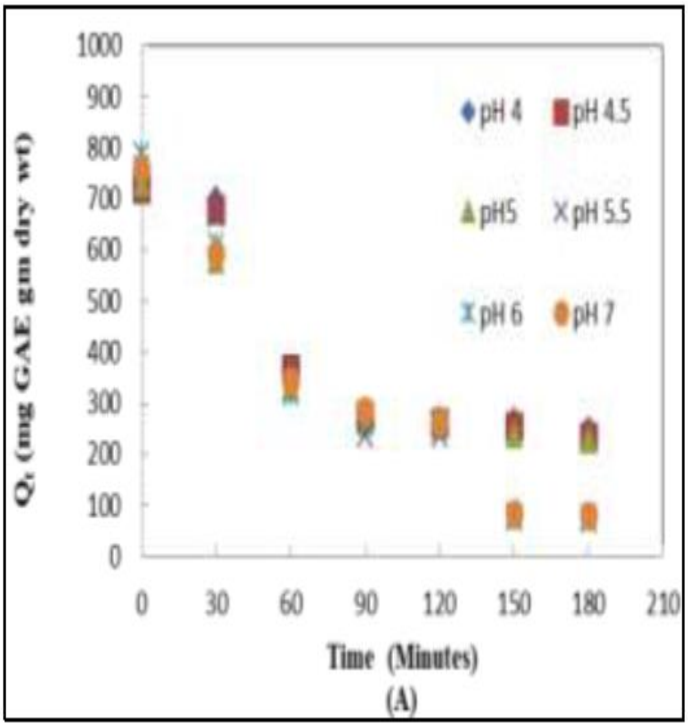
3. RESULTS & DISCUSSION

Batch adsorption

Effect of pH on the Adsorptive Capacity for Batch Adsorption: The pH value of the aqueous solution is an important controlling parameter in any adsorption process.

$$\%\text{ of adsorption} = \frac{q_i - q_t}{q_t} \times 100$$

The pH value can affect the process by affecting the surface charge of adsorbent, the degree of ionization and speciation of adsorbate during adsorption. Thus, the effect of pH in the solution on the adsorption percentage of polyphenol on amberlite IR 400 resin was studied at a pH range of 4.0-7. The experiment was performed with an initial polyphenol concentration of 5.65 mg/ml, at 25°C with a contact time of 180 minutes [5]



(A)

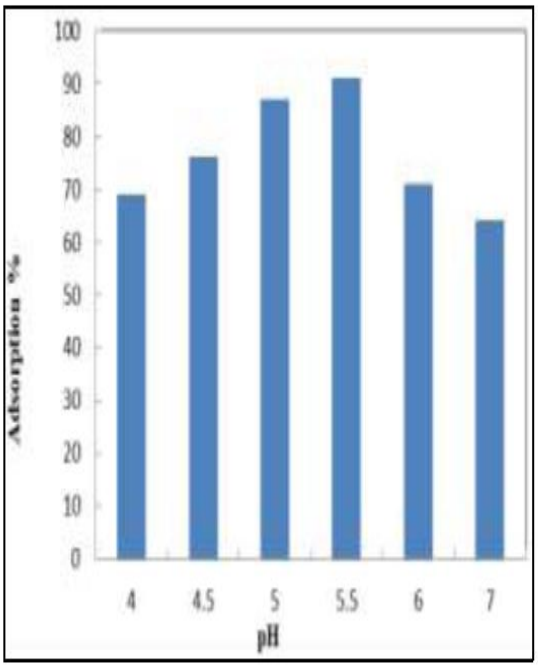
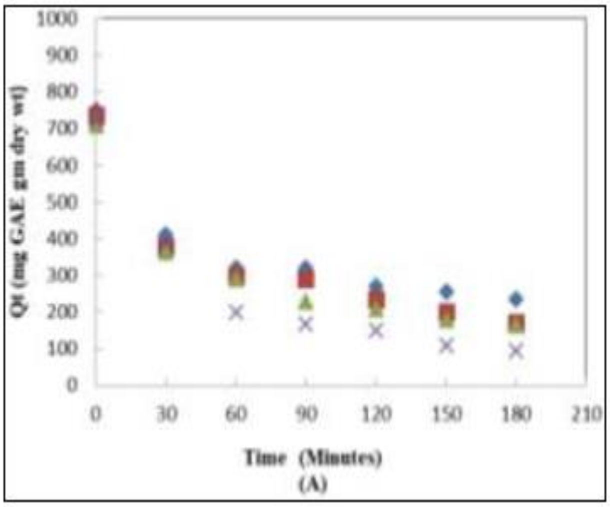


Fig. 1: (A) Kinetic Curve on Adsorptive Capacity in pH range of 4.0-7, (B) Effect of pH on Adsorption Percentage (%)

Effect of Temperature for Batch Adsorption: Temperature is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.65 mg/ml was treated. Observation of effect of temperature on adsorption percentage (%) and kinetic curve of adsorptive capacity of pomegranate peel on amberlite IR-400 resin in the for temperature ranging from 25°C to 40°C pomegranate peel. It was observed that maximum of the gallic acid was absorbed by resin in first one and half hour from initialization of adsorption. It was also observed that temperature of solution has an effect on adsorption process [5].



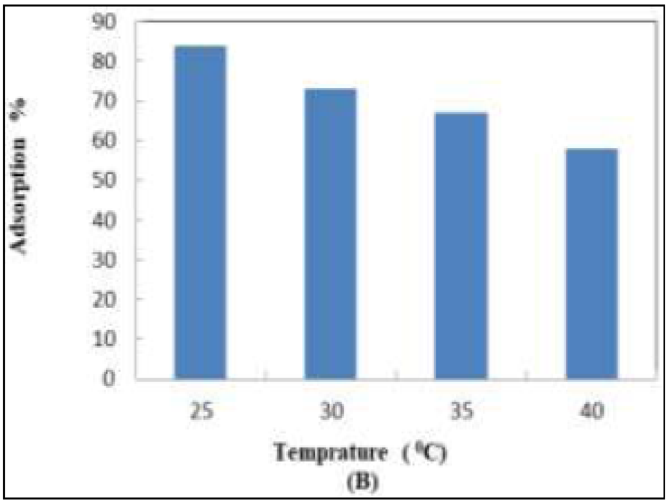


Fig. 2: (A) Kinetic Curve on Adsorptive Capacity in the RPM Range of 30-120 RPM, and (B) Effect of RPM on Adsorption Percentage (%)

Effect of RPM for Batch Adsorption: Speed of agitation is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.0 mg/ml was treated with the 10 g of resin for 180 minutes at RPM ranging from 30 rpm to 120 rpm.

Effect of Temperature for Continuous Adsorption

Temperature is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.65 mg/ml was treated with the 10 g of resin for 180 minutes at temperature ranging from 25°C to 40°C.

Observation of Effect of Temperature on adsorption percentage (%) and Kinetic curve of adsorptive capacity of pomegranate peel on amberlite IR-400 resin in the Temperature range of 25-40 0C for pomegranate peel: The gradual decreases in gallic acid adsorption percentage indicate the exothermic nature of the adsorption process. To avoid compound loss, plant extracts prepared at elevated temperature should be cooled before applying to adsorption columns.

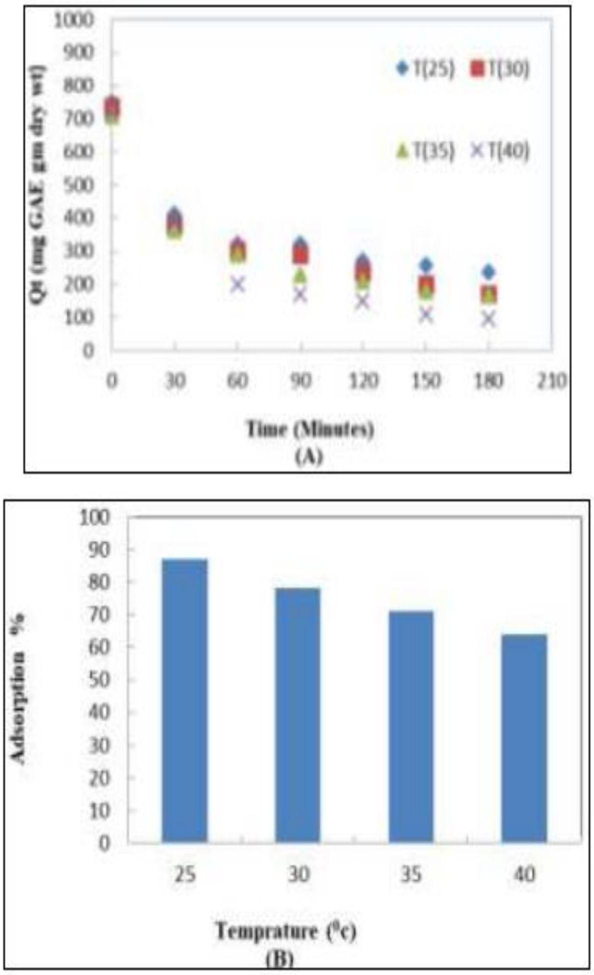


Fig. 3: (A) Kinetic curve on adsorptive capacity in the temperature of range 25-40 0C, and (B) Effect of Temperature on adsorption percentage (%)

4. CONCLUSION

The above work was carried out to get a better understanding on how the processing parameters can be manipulated for optimization of adsorption based purification of pomegranate peel for gallic acid. The present study of biosorption of gallic acid on an ion exchange resin shows that the adsorption process is dependent on the pH, temperature, rpm and concentration of the solution. The adsorption capacity was low at slightly acidic medium (pH 4.0) and gradually increased with increasing pH values up to pH 5.5., adsorption percentage of total polyphenol decreases with increasing temperature, adsorption percentage have less effect on change in rpm but increases with increase in rpm, for concentration in increases gradually with increase in concentration up to equilibrium and the decreases. Adsorption capacity was highest at 25°C and gradually decreased with increase in temperature indicating the exothermic nature of adsorption. It was found that at pH 5.5 and 25°C temperature, the adsorption of total polyphenol by Amberlite IR-400 was found maximum.

REFERENCES

1. Kammerer D. R., Saleh Z. H., Carle R. & Stanley R. A. (2007)“Adsorptive recovery of phenolic compounds from apple juice”. European Food Research & Technology, pp 605-613.
2. Navindra Seeram, P., N. Risa Schulmann and D. Heber. (2006) “Pomegranates: Ancient Roots t Modern Medicine.” CRC. Press. Boca Raton, FL, USA.
3. Konczak, I.; Zabaras, D.; Dunstan M. and Aguas, P. (2010). “Antioxidant capacity and phenolic compounds in commercially grown native Australian herbs and spices”. Food Chemistry, 122 (1): 260-266.
4. J.G. Gujar,S.J. Wagh, V.G. Gaikar (2010).“Experimental and modeling studies on microwave-assisted extraction of thymol from seeds of Trachyspermum ammi (TA) ” Sep. Purif. Technol.70 (3), pp.257–264.
5. Li P., Wang Y., Ma R. & Zhang X. (2005) “Separation of tea polyphenol from green Tea leaves by a combined CATUFMadsorption resin process”. Journal of Food Engineering, 253-260.
6. Rahman M. & Rafiqul Islam M., (2007) “Effect of pH on isotherms modeling for Cu (II) ions adsorption using maple wood sawdust”, Chemical Engineering Journal, pp 273-280.
7. Chandreyee Datta, Asmita Dutta, Debjani Dutta, Surabhi Chaudhuri, (2011) “Adsorption of polyphenols from ginger rhizomes on an anion exchange resin Amberlite IR-400 – Study on effect of pH and temperature”, Procedia Food Science, pp 893-899.

INTEGRATED NUTRIENT AND PEST MGT (INPM) IS THE PRIME MOVER FOR THE SUSTAINABLE AGRICULTURE

V Janaki[1]., K Amitha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- vjanaki7@gmail.com)

2.Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- kamitha123@gmail.com:-)

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract - Integrated nutrient and pest mgt. (INPM) is the prime mover for the sustainable agriculture. The over dose of fertilizers and unsafe pesticides have led to pollution and serious health issues. Nano science may solve some of the issues by providing nonmaterial of higher performance. An attempt has been made to review the development of Nano fertilizers and Nano pesticides and their influence on crop systems. Nano fertilizers such as N, P, K, Fe, Mn, Zn, Cu, Mo and carbon nanotubes show better release and targeted delivery efficiency. Nano pesticides such as Ag, Cu, SiO2, ZnO and Nano formulations show better broad-spectrum pest protection efficiency in comparison with conventional pesticides.

Key Words: Agriculture, Nanotechnology, Nano fertilizer, Nano pesticide, Pest control.

1. INTRODUCTION

The escalation of the food production for fulfilment of food requirement of increasing population is one of the major challenges in the world. The growth of population is increasing continuously and reached up to 7.37 billion. To overcome this situation, the use of chemical fertilizers and pesticides are being used in farming system from previous five decades. The consumption of total pesticide has increased from 196 to 516 million pounds only in USA.

In reality, the use of chemical fertilizers and pesticide has increased the food production many times but reduced food quality and soil fertility. It has been found that 50 to70% of chemical inputs remains unused by leaching, mineralization and bioconversion. Chemical fertilizers and pesticide residues have affected the human health and also destabilized the sublevels of ecosystem (i.e. soil microbial flora, parasites and marine environment) by runoff and eutrophication (CHIPPA et al 2016).

Therefore there is need to improve conventional farming practices into smart practices by the involvement of advanced technologies like nanotechnology for sustainable agriculture. Nanotechnology is the fifth revolutionary technology of the century after biotechnology. It showed wide application spectrum in many disciplines like agriculture, medicine, biology, physics, chemistry, material science, electronics energy and environment. In this technology, we study nano meter (1–100 nm) size materials and theirs. At Nano scale, material has specific physical, optical, mechanical and chemical characteristics in comparison with their bulk form.

Nanotechnology is the emerging technology of this decade and can be a prominent application in agriculture sector (Chhipa and Joshi 2016). The Nano tools in the form of Nano fertilizer and Nano pesticide have been modifying conventional farming practices into precision farming. Different types of nanoparticles such as carbon nanotubes, Cu, Ag, Mn, Mo, Zn, Fe, Si, Ti, their oxides, and nano formulations of conventional agricultural inputs like phosphorus, urea, sulphur, validamycin, tebuconazole and azadiractina have been converted into Nano pesticide and Nano fertilizer.

Nano form has shown results within optimum concentration on seed germination, plant growth and production. Similarly, nano pesticides have displayed positive impact on control of plant pest and disease (Kashyap et al. 2015; Parisi et al. 2014; Delfani et al. 2014). Nano forms deliver active ingredient to the plant by encapsulation inside nanomaterial or within Nano porous material, Nano coating by polymers and Nano emulsion or nanoparticle form (DeRosa et al. 2010).

It is hypothesized that Nano tools performed controlled release capacity of agriculture inputs which could be helpful in maintaining eco balance and provide sustainable solutions to climate change and environmental pollution. The site-specific and controlled release of active ingredients of agricultural inputs reduces the amount and cost of fertilizer and pesticide expense on farmers.

2. NANOTECHNOLOGY IN AGRICULTURE

Nanotechnology has potential for sustainable agriculture practice. It is expected that it will lead towards precision farming. Precision farming aims for improved crop yield improvement by monitoring environmental variables and applying controlled target action for a situation (Chen and Yada 2011).

The use of Nano formulation, Nano encapsulation and functionalized nanomaterial of next-generation fertilizers and pesticides provides site-specific and controlled delivery of active ingredients (fertilizers and pest protectant) to plants and reduces excess run-off (Nair et al. 2010; Ghormade et al. 2011; Khot et al. 2012).

The development of smart delivery system in the form of Nano fertilizer, Nano pesticide, Nano herbicide and Nano sensor has been open up new mode of applications for sustainability of agricultural sector (Scott and Chen 2013).

Nano-fertilizer

Nano-fertilizer are Nano-materials, responsible for providing one or more types of nutrients to the growing plants, and support their growth and improve production (Liu and Lal 2015). Based on plant nutrient requirement, nano fertilizer is divided into following categories (A) macro- and (B) micro-Nano-fertilizer, (C) Nano particulate fertilizer

1.2 Macro-Nutrient Nano-fertilizerz

Nutrient is required in large amount in traditional farming practices. Nitrogen (N), phosphorus (P), potassium (K), magnesium (Mg), sulphur (S) and calcium (Ca) are as macronutrients for plant growth. Increasing food production demand may push up macronutrient fertilizer requirement up to 263 MT by 2050 (Alexandratos and Bruinsma 2012).

High-volume-to-surface ratio of nanomaterial reduces the amount and increases the efficiency of macronutrient Nano-fertilizer in comparison with traditional fertilizers. In this regard, many researchers have developed macronutrient Nano-fertilizer and used this at laboratory and field scale. Liu and Lal (2015) and Ditta et al. (2015) have reviewed the use of Nano-fertilizer in agriculture. Urea-coated zeolite chips and urea-modified hydroxyapatite nanoparticles have been synthesized as a source of N shown their capabilities as slow and controlled release of N for long time period (Millan et al. 2008; Kottegoda et al. 2011). Further, Delfani et al. (2014) developed Mg NP as alternate of Mg and found 7% increment in Vigna unguiculata seed weight.

3. MICRONUTRIENT NANO-FERTILIZER

Micronutrients are trace element which is required in minute quantity (B100 ppm) but essential for different metabolic processes in plants. Nano form of micronutrients improves their bioavailability to the plants and shows a significant improvement in plant growth and nutrition quality.

In this regard, Delfani et al. (2014) used Fe NP on blacked eyed pea and measured 10% increment in chlorophyll content in leaves. Similarly, in G. max chlorophyll content was increased by Fe NP at 30–60 ppm concentration (Ghafariyan et al. 2013). Spray of Mn NP on Vigna radiate increased 52% root length, 38% shoot length 71% rootlet and 38% biomass at 0.05 ppm concentration in comparison with bulk MnSO4. Zinc is the essential micronutrient and regulates the different enzymatic activities in plants. ZnO NP showed a significant improvement in biomass, shoot length, root, chlorophyll and protein content, and phosphate enzyme activity in Vigna radiate, Cicer ariatium, Cucumis sativas,

Raphanus sativus, Brassica napus and Cluster bean (Zhao et al. 2013; Raliya and Tarafdar 2013). In the case of copper, Cu NP improved photosynthesis in Elodea desaplanch by 35% at low concentration (Nekrasova et al. 2011) and seeding growth up to 40% in lettuce (Shah and Belozerova 2009). Molybdenum nanoparticle also showed improved microbial activity and seed growth in chickpea after combined treatment with nitrogen fixation bacteria (Taran et al. 2014).

4. RESULT & DISCUSSION

Currently, Nano-agriculture is focusing on target farming that applies Nano-sized particles with unique properties to boost crop production (Batsmanova et al. 2013; Scott and Chen 2013). In the traditional practices, seed germination, plant growth promotion and crop improvement are now being reported successfully replaced by the application of carbon nanotubes as regulators of seed germination and plant growth (Khodakovskaya et al. 2013; Zheng et al. 2005). The use of Nano-sized bacteriophages has also shown promising biological alternatives to conventional Cu bactericides. Small in size and high-surface-to-volume ratio character of nanoparticles make them more efficient in comparison with their bulk components.

Engineered nanoparticles enter into intercellular space through Apo plastic pathway.

Further, through Apo plastic (through cell wall), particles may enter into epidermal and cortical cell to reach endodermis and accumulate uniformly or as aggregate form (Zhao et al. 2013b). In contrast Rico et al. (2011) hypothesized that simplistic (through cytoplasm) route is a more organized and regulated pathway for movement of engineered nanoparticles into plants. They proposed that binding of nanoparticle with carrier protein is helpful in cell internalization and easy to move through ion channels, aquaporin's and endocytosis.

5. CONCLUSION

Nanotechnology has opened an new domain in agricultural practices that can provide sustainable tools to conventional farming practice in the form of Nano-fertilizer and Nano-pesticide. Nano form of conventional agriculture -inputs provides the site-specific and controlled release of active ingredient that can reduce the excess run-off and prevent eutrophication and residual contamination. The use of encapsulated and metal Nano-fertilizer and Nano-pesticide has been evidenced their promising approach in agriculture. Ca and P hydroxyapatite, Fe, ZnO, TiO2, Ag nanoparticles and CNT can be used as an alternate of conventional agriculture-input. Further, more research is required in environment impact assessment of Nano-tools before commercialization.

REFERENCES

1. Agrawal S, Rathore P (2014) Nanotechnology pros and cons to agriculture: a review. Int Curr Microbiol App Sci 3:43–55. doi:10.13140/2.1.1648.1926
2. Chhipa H, Joshi P (2016) Nanofertilisers, nanopesticides and nanosensors in agriculture. In: Ranjan S, Dasgupta N, Lichtfouse E (eds) Nanoscience in food and agriculture 1, Sustainable agriculture reviews, vol 20. Springer, pp 247–282. doi:10.1007/ 978-3-319-39303-2
3. Lal R (2015) Potentials of engineered nanoparticles as fertilizers for increasing agronomic productions. Sci Total Environ 514:131–139. doi:10.1016/j.scitotenv.2015.01.104
4. Liu X-M, Feng Z-B, Zhang S-Q, Zhang F-D, Zhang J-F, Xiao Q, Wang Y-J (2006) Preparation and testing of cementing nanosubnano composites of slower controlled release of fertilizers. Sci Agric Sin 39:7
5. Lu C, Zhang C, Wen J, Wu G, Tao M (2002) Research of the effect of nanometer materials on germination and growth enhancement of Glycine max and its mechanism. Soybean Sci 21:168–171
6. Mukhopadhyay SS (2014) Nanotechnology in agriculture: prospects and constraints. Nanotechnol Sci Appl 7:63. doi:10.2147/NSA. S39409
7. Nair R, Varghese SH, Nair BG, Maekawa T, Yoshida Y, Kumar DS (2010) Nanoparticulate material delivery to plants. Plant Sci 179:154–163. doi:10.1016/j.plantsci.2010.04.012
8. Pradhan S, Patra P, Das S, Chandra S, Mitra S, Dey KK, Akbar S, Palit P, Goswami A (2013) Photochemical modulation of biosafe manganese nanoparticles on Vigna radiata: a detailed molecular, biochemical, and biophysical study. Environ Sci Technol 47:9. doi:10.1021/es402659t
9. Ditta A, Arsha, M, Ibrahim M (2015) Nanoparticles in sustainable agricultural crop production: applications and perspectives. In: Nanotechnology and plant sciences. Springer International Publishing, pp 55–75. doi:10.1007/978-3-319-14502-0_4
10. Gopal M, Gogoi R, Srivastava C, Kumar R, Singh PK, Nair KK et al (2011) Nanotechnology and its application in plant protection. In: Thind TS et al (eds) Plant pathology in India: vision 2030. pp 224–230

INVESTIGATE THE CORROSION BEHAVIOR OF ALUMINUM METAL MATRIX COMPOUNDS (MMC) REINFORCED WITH BERYL 6061 PARTICLES

Dr P Geetha[1]., V Janaki[2]

1 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- pgeetha123@gmail.com)

2.Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- vjanaki7@gmail.com)

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract

The aim of the research was to investigate the corrosion behavior of aluminum metal matrix compounds (MMC) reinforced with beryl 6061 particles in a mixture of alkaline and saline solutions using the weight loss method. The mixture of saline and alkaline solution used is a mixture of sodium hydroxide and sodium chloride solutions. Composite materials are made using the technique of liquid metallurgy using the vortex method. 6061 aluminum / beryl particles MMCs with 2, 4 and 6 wt .-% beryl particles are cast. The corrosion properties of aluminum, the 6061 / beryl particle compound and the unreinforced alloy were evaluated experimentally. The corrosion test was carried out at different concentrations of the mixture of sodium hydroxide and sodium chloride solution in a concentration of 0.025 M, 0.05 M and 0.1 M solutions for different exposure times. The results indicated that the corrosion rate of the metal matrix composites under the corrosive atmosphere was lower than that of the 6061 aluminum matrix material regardless of exposure time and concentration of the corrosive material. Aluminum The 6061 / beryl particle compound becomes more corrosion-resistant as the beryl content increases. This is due to the formation of a stable layer on the samples. Scanning electron microscopy (SEM) shows the degree of attack of the alkaline solution on the surface of the material being examined.

Keywords: Beryl particulates, Corrosion loss, Metal Matrix Composite (MMCs), Weight loss.

1. INTRODUCTION

Metal matrix composites are an important class of materials that contain metal or alloys as a matrix and ceramic or fiber particles or whiskers as reinforcements. Metal matrix composites based on aluminum have increased resistance to corrosion, wear and mechanical properties. They offer significantly improved properties on metals and alloys. They are used for aerospace, power, automotive, and military applications 1-2. Short fiber reinforced MMCs offer exceptional specific strength and stiffness along the fiber direction compared to those with particle reinforcements, which have more isotropic properties. Most of the research on particle reinforced MMCs has focused on their 3-4 mechanical and manufacturing properties. Little research has been done into their corrosion behavior, which is why the corrosion mechanisms are not well understood. There are conflicting interpretations and data on fundamental issues such as the locations of corrosion initiation and the role of reinforcement in susceptibility to corrosion. Corrosion can affect the metal matrix composite in a number of ways, depending on its type and the prevailing environmental conditions. Studying the corrosion resistance of Al-based materials is particularly important for automotive and aerospace applications. The main advantages of 6061 aluminum composites over unreinforced materials are: superior strength, improved stiffness, reduced density, good corrosion resistance, improved high temperature properties, controlled coefficient of thermal expansion, heat / thermal management, improved wear resistance and improved damping capabilities5-6. One of the main disadvantages of using metal matrix composites is the influence of reinforcement on the rate of corrosion. This is particularly important for connections based on aluminum alloys, where a protective oxide film ensures corrosion resistance. The present work focuses on the corrosion properties of 6061 aluminum / beryl metal matrix compounds.

2. SELECTION OF MATERIALS AND METHODS

The material selected for this research is the commonly used 6061 aluminum alloy, which is commercially available. Its composition is given in Table 1.

Table - 1
Composition of Aluminium 6061 alloy

Mg	*Si*	*Fe*	*Cu*	*Ti*	*Pb*
0.8-1.5	*10-12*	*1*	*0.7-1.5*	*0.2*	*0.1*

The media used for the corrosion tests are mixtures of 0.025 M, 0.05 M and 0.1 M sodium hydroxide solution and sodium chloride. The method used to characterize corrosion is the weight loss static corrosion method according to ASTM G69-80. The composites are made according to the liquid fusion metallurgy technique used by Krupakara et al9. Preheated uncoated beryl particles are added to the molten 6061 aluminum alloy. Compounds are made containing 2, 4, and 6 weight percent beryl particles. For comparison, the aluminum alloy 6061 was also cast. The molded parts are in the form of a cylindrical rod. The sample is made from the molded rod parts. Cylindrical samples measuring 20 mm x 20 mm are machined from the cast rod parts of the composite materials and the matrix alloy. All samples are subjected to standard metallographic techniques as performed by S. EzhilVannan and Paul Vizhian Simson10 prior to the static weight loss corrosion test.

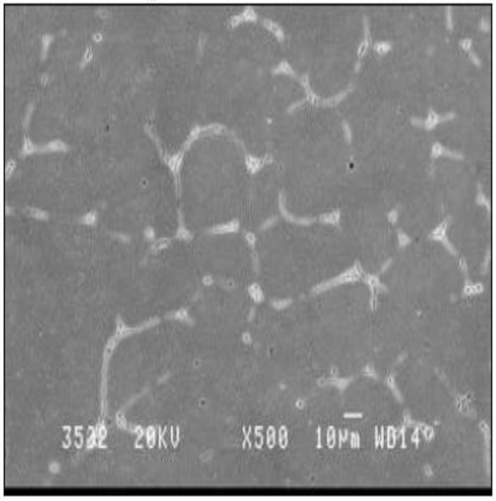


Fig. 1: Microstructure of Matrix

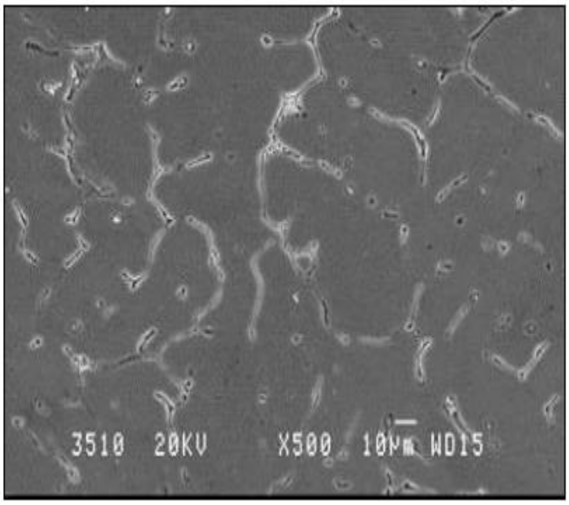


Fig. 2: Microstructure of 2 % composite

3. RESULTS AND DISCUSSIONS

The results of the weight loss corrosion tests on various mixtures of concentrated sodium hydroxide and sodium chloride solutions are shown in Figures 3-4.

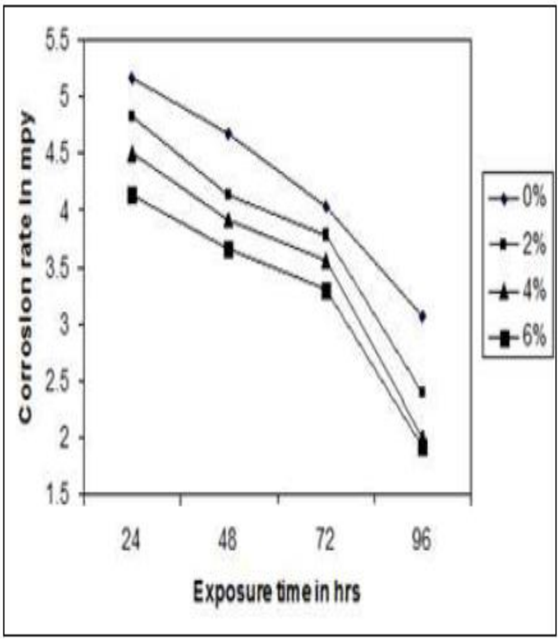


Fig. 3: Results of the test in 0.025M mixture

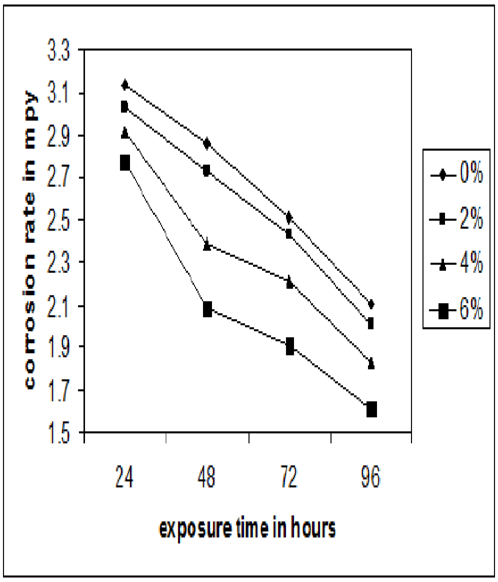


Fig. 4: Results of the test in 0.05M mixture

Figures 5 to 7 show the results obtained for the static weight loss corrosion test of compounds composed of 6061 aluminum / beryl particles and the matrix alloy in mixtures of 0.025 M, 0.05 M and 0.1 m, respectively, for different exposure times. The results can be discussed under the topic Effect of exposure time and Effect of beryl particle content.

4. EFFECT OF EXPOSURE TIME

The trend observed in all cases shows a decrease in corrosion with increasing test duration. The graphs show that the corrosion resistance of the composite increases with increasing exposure time. This eliminates the possibility of hydrogen bubbles sticking to the surface of the sample and forming a permanent layer that affects the corrosion process. The phenomenon of a gradual decrease in the corrosion rate indicates a possible passivation of the matrix alloy. De Salazar11 explained that the black protective film consists of hydroxychloride hydrogen, which previously slows down the reaction. Lock and. al.12 pointed out that the black film consists of a compound of aluminum hydroxide. This layer protects against corrosion even in acidic environments. However, the exact chemical nature of such a protective film has not yet been determined. It can be clearly seen in FIGS. 6 to 8 that in the case of cast iron and composite material the corrosion rate decreases monotonically with increasing beryl particle content. In this case, the corrosion rate of the composite materials as well as the matrix alloy is mainly due to the formation of pitting and cracks on the surface. In the case of the base alloy, the resistance of the corrosion medium used leads to the formation of cracks on the surface, which ultimately leads to the formation of pits and thus the loss of material. The presence of cracks and pitting on the surface of the base alloy was clearly observed. Since no reinforcement is provided in any way, the base alloy offers no resistance to acids. Therefore, the weight loss with an unreinforced alloy is greater than with composite materials.

5. CONCLUSIONS

The content of beryl particles in 6061 aluminum alloys plays an important role in the corrosion resistance of the material. Increasing the percentage of beryl particles is beneficial to decrease the density and increase the strength of the alloy, but therefore the corrosion resistance is greatly increased. Aluminum 6061 MMC, when reinforced with 0 to 6 wt% beryl particles, could be successfully produced by the technique of molten metallurgy. The rate of corrosion of the alloy and composite decreased with time for all concentrations of sodium hydroxide and sodium chloride solutions. The corrosion rate of the composites was lower than that of the matrix alloy according to the concentrations of sodium hydroxide and sodium chloride solution. Composites are better suited than alloys for applications in alkaline and marine environments.

REFERENCES

1. A Vassel, Continuous fibre reinforced titanium and aluminium composites: A comparison, Mater. Sci. Eng. A 263 (1999) 305-313.
2. T.P.D. Rajan, R.M. Pillai, B.C. Pai, Reinforcement coatings and interfaces in aluminium metal matrix composites, J. Mater. Sci. 33 (1998) 3491-3503.
3. J. Rodel, H. Prielipp, M. Knechtel, N. Claussen, Better ceramics through metal modification, Trans. Mater. Res. Soc. Jpn. 19B (1994) 763-776.
4. S. EzhilVannan and Paul Vizhian Simson, Corrosion Behaviour of Short Basalt Fiber Reinforced with Al7075 Metal Matrix Composites in Sodium Chloride Alkaline Medium, J. Chem. Eng. Chem. Res.1(2), (2014), 122-131.
5. J.M.G.DeSalazar, A.Urefia, S.Mazanedo and M.Barrens, Corrosion behaviour of AA6061 and AA7075 reinforced with Al2O3 particulates in aerated 3.5%chloride solution potentiodynamic measurements and microstructure evaluation, Corrosion Science, 41, (1999), 529-545.
6. J.F.Mclyntyre, R.K.Conrad&S.L.GoHedge, "Technical note: The effect of heat treatment on the pitting behaviour of SiC / AA2124", Corrosion, vol 46,190-192.

STUDY AND PURIFICATION OF NATURAL POLYPHENOLS (GALLIC ACID)

K Amitha[1]., Dr. P Geetha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- :- kamitha123@gmail.com)

2.Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉:- pgeetha123@gmail.com:-)

Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India.

Abstract

Gallic acid is an interesting natural compound because of its antioxidant, anti-inflammatory, antifungal and antitumor properties. It is present in relatively high concentrations in a number of biomass sources and in industrial wastes from where it could be extracted. Aiming at developing benign and efficient extraction and purification processes for gallic acid, aqueous two-phase systems (ATPS) composed of ionic liquids (ILs) and inorganic salts were investigated. The present investigation was focused on improving the feasibility of large scale applications of a solid phase extraction (SPE) procedure dedicated to the recovery of polyphenols. Adsorption of polyphenol (gallic acid) on an anion exchange resin, Amberlite IR-400 was studied for purification of polyphenols from the pomegranate peel. The work was carried out to understand how the processing parameters can be manipulated to optimize the purification of gallic acid for its further use in nutraceutical and functional foods. In this work the effect of pH, temperature, speed of agitation and concentration for gallic acid adsorption on anion exchange resin was studied.

Keywords: Resin, Antioxidant, Gallic Acid, Extraction, Adsorption, Separation.

1. INTRODUCTION

Pomegranate belongs to Punicaceae family. Punica granatum (Punicaceae), commonly called pomegranate, recently described as nature’s power fruit, is a plant used in folkloric medicine for the treatment of various diseases. The Pomegranate has strong antioxidant and anti-inflammatory properties, recent studies have demonstrated its anti-cancer activity in several human cancers. In addition, pomegranate peel extract with an abundance of gallic acid flavonoids and tannins has been shown to have a high antioxidant activity. Antimicrobial drug resistance in human bacterial pathogens is a worldwide issue and as a consequence, effective treatment and control of such organisms remain an important challenge. The chemical formula is C6H2(OH)3COOH. Gallic acid is found both free and as part of tannins. Salts and esters of gallic acid are termed 'gallates'. Despite its name, it does not contain gallium. Gallic acid is commonly used in the pharmaceutical industry. Gallic acid can also be used as a starting material
in the synthesis of the psychedelic alkaloid mescaline .Gallic acid seems to have anti-fungal and anti-viral properties. Gallic acid acts as an antioxidant and helps to protect human cells against oxidative damage. Gallic acid was found to show cytotoxicity against cancer cells, without harming healthy cells. Gallic acid is used as a remote astringent in cases of internal haemorrhage. Gallic acid is also used to treat albuminuria and diabetes. Gujar et al 2010 [1] has extensively studied extraction of catachin and epicatechin from Indian green tea leaves. The detailed study of effect of various operating parameters has been studied in the current work. The effect of microwave irradiation on thymol extraction shows increase in the percentage extraction of thymol from ajowain seed [2]. This present work deals with extraction and purification Gallic acid from peel of pomegranate to use it to biological and chemical test as standard compound by resin adsorption.

2. EXTRACTION OF GALLIC ACID

Materials & Methods

Instruments: Lab equipment was provided by Aavanira Biotech Private Limited, absorbance measurements was made on Thermo UV/Visible spectrophotometer with a pair of matched quartz cells of 1 cm width, Elder digital balance used for weighing.

Materials: All Raw materials purchased from local Market Pune. All the chemicals and reagents were of analytical grade and were purchased from Gandhi chemicals and Bioresource life science.

Selection of Common Solvent: After assessing the solubility of polyphenol in different solvents Ethanol has been selected as common solvent for developing spectral characteristics.

Soxhlet Extraction

Soxhlet extraction is a procedure for extracting nonvolatile and semi volatile organic compounds from solids such as dry powder, peel, soils, sludge's, and wastes. The Soxhlet extraction process ensures intimate contact of the sample matrix with the extraction solvent.

Preparation of Pomegranate Peel Extract

10 gm of pomegranate peel was used with 500 ml of ethanol and kept in an extraction thimble. The extraction thimble drained freely for the duration of the extraction period with the condenser attached to the top of the soxhlet apparatus. Soxhlet extraction was conducted for about 8 hours and the crude extract was used as a raw material for adsorption. The maximum amount of gallic acid is 0.35 mg/10 gm of peel of pomegranate.

Pretreatment of Adsorbent

10 gm of anion exchange resin Amberlite IR 400 was weighed and taken in a 250 ml conical flask. The adsorbent was washed with distilled water, then with 15 times w/v 0.5 (N) HCl and 0.5 (N) NaOH, and finally again with distilled water till neutral pH was obtained.

Batch & Continues Adsorption Study

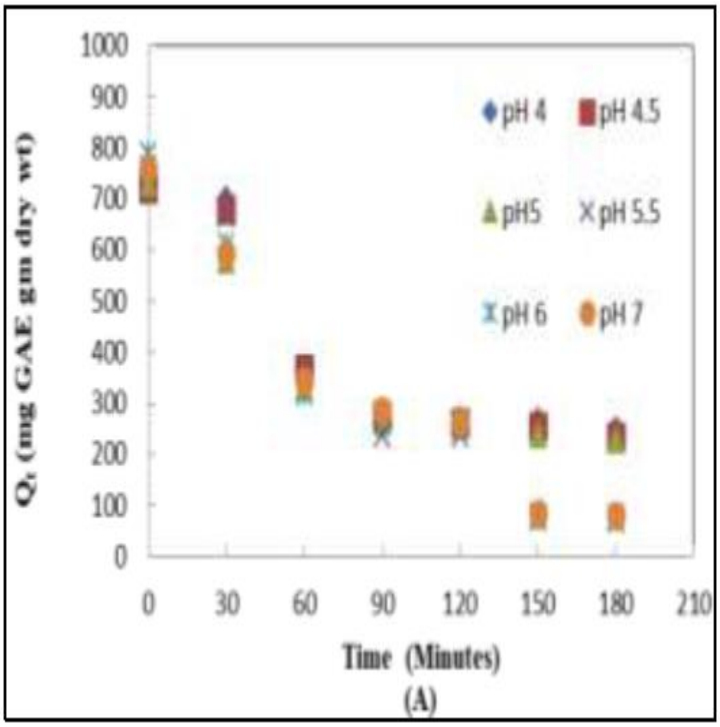
10 g of pretreated resin suspended in buffer was kept in a 250 ml of conical flask. 50 ml of pomegranate peel extract (in 50% aqueous-ethanolic solution) with known polyphenol concentration was added to each flask. The flasks were kept in a shaking incubator maintained at 120 rpm and 25°C until adsorption equilibrium was reached. The temperature range was varied from 25-40°C, and pH of the buffer solution was varied from 4-7. The buffer pH of 4-5.5 were obtained using citrate buffer (an equimolar (0.1 M) mixture of citric acid and tri-sodium citrate). For pH 6-6.5, phosphate buffer (an equimolar (0.2 M) mixture of sodium dihydrogen phosphate and di-sodium hydrogen phosphate) were used. The adsorptive capacity of the resin is represented by the following expression. [3]

$$\% \text{ of adsorption} = \frac{q_i - q_t}{q_t} \times 100$$

3. RESULTS & DISCUSSION

Batch adsorption

Effect of pH on the Adsorptive Capacity for Batch Adsorption: The pH value of the aqueous solution is an important controlling parameter in any adsorption process. The pH value can affect the process by affecting the surface charge of adsorbent, the degree of ionization and speciation of adsorbate during adsorption. Thus, the effect of pH in the solution on the adsorption percentage of polyphenol on amberlite IR 400 resin was studied at a pH range of 4.0-7. The experiment was performed with an initial polyphenol concentration of 5.65 mg/ml, at 25°C with a contact time of 180 minutes [5]



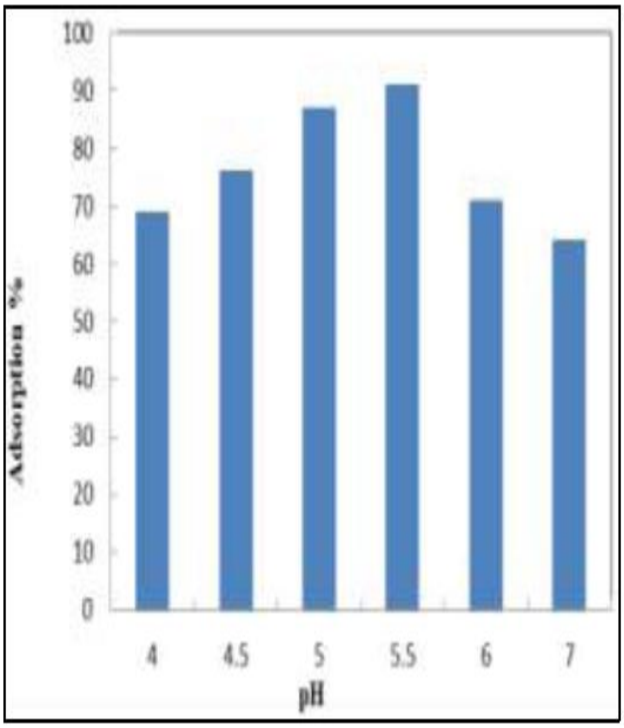


Fig. 1: (A) Kinetic Curve on Adsorptive Capacity in pH range of 4.0-7, (B) Effect of pH on Adsorption Percentage (%)

Effect of Temperature for Batch Adsorption: Temperature is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.65 mg/ml was treated. Observation of effect of temperature on adsorption percentage (%) and kinetic curve of adsorptive capacity of pomegranate peel on amberlite IR-400 resin in the for temperature ranging from 25°C to 40°C pomegranate peel. It was observed that maximum of the gallic acid was absorbed by resin in first one and half hour from initialization of adsorption. It was also observed that temperature of solution has an effect on adsorption process [5].

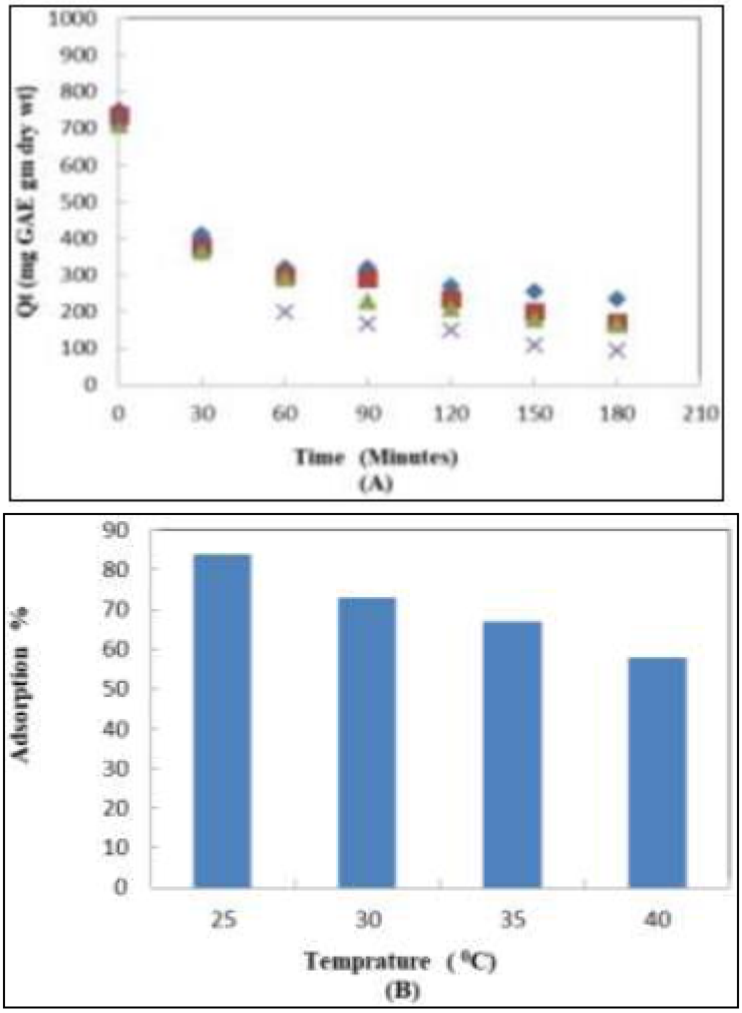


Fig. 2: (A) Kinetic Curve on Adsorptive Capacity in the RPM Range of 30-120 RPM, and (B) Effect of RPM on Adsorption Percentage (%)

Effect of RPM for Batch Adsorption: Speed of agitation is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.0 mg/ml was treated with the 10 g of resin for 180 minutes at RPM ranging from 30 rpm to 120 rpm.

Effect of Temperature for Continuous Adsorption

Temperature is also one of the major factors affecting the biosorption process. In this study, 50 ml of polyphenol solution with initial polyphenol concentration of 5.65 mg/ml was treated with the 10 g of resin for 180 minutes at temperature ranging from 25°C to 40°C.

Observation of Effect of Temperature on adsorption percentage (%) and Kinetic curve of adsorptive capacity of pomegranate peel on amberlite IR-400 resin in the Temperature range of 25-40 0C for pomegranate peel: The gradual decreases in gallic acid adsorption percentage indicate the exothermic nature of the adsorption process. To avoid compound loss, plant extracts prepared at elevated temperature should be cooled before applying to adsorption columns.

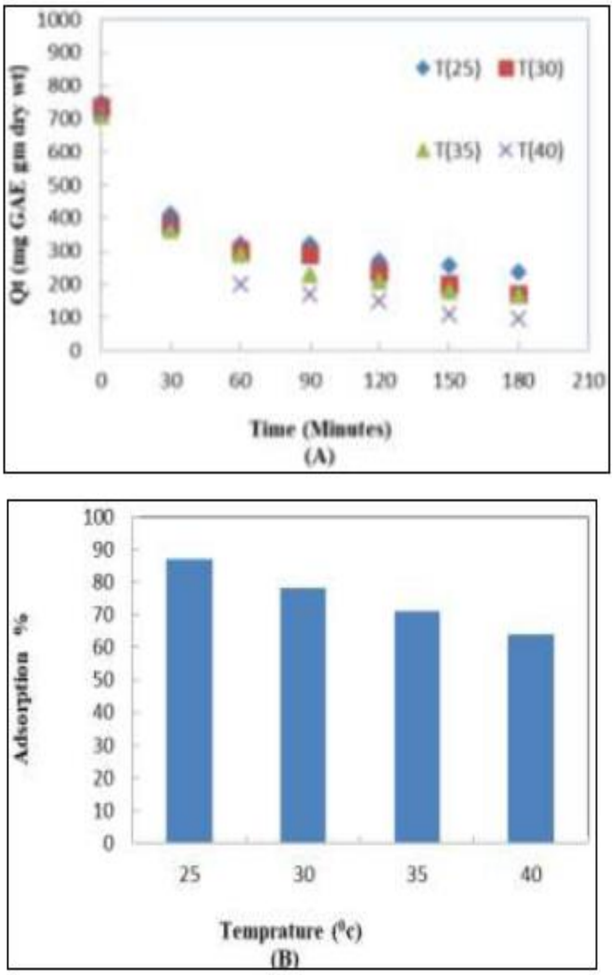


Fig. 3: (A) Kinetic curve on adsorptive capacity in the temperature of range 25-40 0C, and (B) Effect of Temperature on adsorption percentage (%)

4. CONCLUSION

The above work was carried out to get a better understanding on how the processing parameters can be manipulated for optimization of adsorption based purification of pomegranate peel for gallic acid. The present study of biosorption of gallic acid on an ion exchange resin shows that the adsorption process is dependent on the pH, temperature, rpm and concentration of the solution. The adsorption capacity was low at slightly acidic medium (pH 4.0) and gradually increased with increasing pH values up to pH 5.5., adsorption percentage of total polyphenol decreases with increasing temperature, adsorption percentage have less effect on change in rpm but increases with increase in rpm, for concentration in increases gradually with increase in concentration up to equilibrium and the decreases. Adsorption capacity was highest at 25°C and gradually decreased with increase in temperature indicating the exothermic nature of adsorption. It was found that at pH 5.5 and 25°C temperature, the adsorption of total polyphenol by Amberlite IR-400 was found maximum.

REFERENCES

1. Kammerer D. R., Saleh Z. H., Carle R. & Stanley R. A. (2007)“Adsorptive recovery of phenolic compounds from apple juice”. European Food Research & Technology, pp 605-613.
2. Navindra Seeram, P., N. Risa Schulmann and D. Heber. (2006) “Pomegranates: Ancient Roots t Modern Medicine.” CRC. Press. Boca Raton, FL, USA.
3. Konczak, I.; Zabaras, D.; Dunstan M. and Aguas, P. (2010). “Antioxidant capacity and phenolic compounds in commercially grown native Australian herbs and spices”. Food Chemistry, 122 (1): 260-266.
4. J.G. Gujar,S.J. Wagh, V.G. Gaikar (2010).“Experimental and modeling studies on microwave-assisted extraction of thymol from seeds of Trachyspermum ammi (TA) ” Sep. Purif. Technol.70 (3), pp.257–264.
5. Li P., Wang Y., Ma R. & Zhang X. (2005) “Separation of tea polyphenol from green Tea leaves by a combined CATUFMadsorption resin process”. Journal of Food Engineering, 253-260.
6. Rahman M. & Rafiqul Islam M., (2007) “Effect of pH on isotherms modeling for Cu (II) ions adsorption using maple wood sawdust”, Chemical Engineering Journal, pp 273-280.
7. Chandreyee Datta, Asmita Dutta, Debjani Dutta, Surabhi Chaudhuri, (2011) “Adsorption of polyphenols from ginger rhizomes on an anion exchange resin Amberlite IR-400 – Study on effect of pH and temperature”, Procedia Food Science, pp 893-899.