ISSN : 2229 - 3515

Volume : 8 ,
Special Issue of NCSCCSS 2018
16-17th November 2018

Proceedings of the
1st National Conference
on
Soft Computing, Communication Systems & Sciences

(NCSCCSS 2K18)

16-17th November 2018

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

1st NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES

(NCSCCSS 2K18)

on

16-17th November 2018

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

Copy Right @ 2018 with the 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.

This book or any part thereof may not be reproduced without the written permission of the Department of Computer Science & Engineering, Department of Electronics & Communication Engineering, MALLA REDDY COLLEGE OF ENGINEERING FOR WOMEN, Maisammaguda, Medchal, Hyderabad-500100, TS, INDIA.

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

Sri. CH. MALLA REDDY

M. P (Malkajgiri – Lokshaba)

Founder Chairman

Message

Now a days the communication technology is developing at a very fast pace. As everyone knows that every country can progress only if the scientists and technocrats explore newer fields of research and development from the bottom of your heart. Software Technology is changing rapidly and new areas of research are coming up. Now it is high time that every one of us will have to think and contribute to the cause. Moreover, there is a growing need for a large scale industry-institute interaction. The faculty members of **MRCEW, HYDERABAD** have rightly sensed this need and provided a good platform for the researchers all around the globe to bring forward their thoughts and help the society at large. **MRCEW, HYDERABAD** has always been a front runner to organize such events and this time too we have come up with NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K18) on 16-17th November 2018.

CH. MALLA 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

Sri. CH.MAHENDER REDDY

Secretary, MRGI

Message

I am indeed very happy that the department of CSE & ECE organizing an NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K18). It will definitely pave way to understand the recent trends and innovations of Soft Computing and Communication Technologies and its applications in industrial and scientific sphere. Imparting the knowledge and exchange views among Teachers and learners should be the basic function of such conference. I hope this conference is going to be a platform for fruitful interaction among the stakeholders. I congratulate the members of the organizing committee of NCSCCSS 2K18 and wish the Conference a Grand 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 an NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K18). The post century made tremendous progress in science and technology laying foundations for modern civilization. The new millennium is galloping into the future with the emerging trends in modern technology for the changing world. To meet this need, it is absolutely essential for the intellectuals of the present, to participate in "Idea Interaction Process" and exchange new technologies for the overall growth of the scientific world, contributing to the process of human race; as a whole. I am confident that this International Conference will go a long way in bringing together the academicians, industry people and researchers in vital areas of Computer Science and Engineering. It will play a definitive role in bringing together researchers, young scientists, and students in an informal environment for discussing the latest trends. 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

Message

It is our great honour to welcome you all the delegates from various parts of the Country to National Conference on Soft Computing, Communication Systems & Sciences (NCSCCSS 2K18). We are very much delighted to note that the overwhelming response for our Invitation from the Authors, Research Scholar, and Industries for this Conference. The Technical Program Committee and Reviewers worked with excellence in selecting high quality papers for oral presentation in the conference and inclusion in the Conference proceedings. We are very glad to have a great response from the Listeners to participate in the Conferences and get the knowledge over the recent trends in the field of Computer & Communication Technologies. We sincerely hope that NCSCCSS 2K18 provides an excellent open forum to exchange ideas and latest research accomplishments among academia and industries, and also to cultivate mutual friendships among professionals in computing domain.

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

Message

It is our great honour to welcome you all the delegates from various parts of the Country to National Conference on Soft Computing, Communication Systems & Sciences (NCSCCSS 2K18). We are very much delighted to note that the overwhelming response for our Invitation from the Authors, Research Scholar, and Industries for this Conference. The Technical Program Committee and Reviewers worked with excellence in selecting high quality papers for oral presentation in the conference and inclusion in the Conference proceedings. We are very glad to have a great response from the Listeners to participate in the Conferences and get the knowledge over the recent trends in the field of Computer & Communication Technologies. We sincerely hope that NCSCCSS 2K18 provides an excellent open forum to exchange ideas and latest research accomplishments among academia and industries, and also to cultivate mutual friendships among professionals in computing domain.

DR. ARCHEK PRAVEEN KUMAR

INTERNATIONAL JOURNAL OF ADVANCES IN SOFTCOMPUTING TECHNOLOGY

(ISSN NO: 2229-3515)

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

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 NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES (NCSCCSS 2K18) on 16-17th November 2018. 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

 # A-905, 2nd Floor, Allwyn Colony, Phase 2, Kukatpally, Hyderabad -72, AP, INDIA

☎ :91-9966023477, ✉ : editor@ijasct.com; www.ijasct.com

1st NATIONAL CONFERENCE ON SOFT COMPUTING, COMMUNICATION SYSTEMS & SCIENCES

(NCSCCSS 2K18)

on

16-17th November 2018

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

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

Editorial Board

Mr. Ch. V. Krishna Mohan	MRCEW Hyderabad
Mr. A. Brahma Reddy	MRCEW Hyderabad

Co-Conveners

Dr. I. Selvamani	MRCEW Hyderabad
Mr. K. G. N. Kumar	MRCEW Hyderabad

Organizing Committee

1	Dr.JOSEPH PRAKASH MOSIGANTI	MRCEW Hyderabad
2	Dr JAYAPRAKASH CHINNADURAI	MRCEW Hyderabad
3	Dr.NELSON JALADANKI	MRCEW Hyderabad
4	Dr JANARDHAN ANTHARAM	MRCEW Hyderabad
5	Mrs. SUJATHA GODAVARTHI	MRCEW Hyderabad
6	Mrs. SUNEETA NETALA	MRCEW Hyderabad
7	Mrs. JONNALAGADDA SRAVANI	MRCEW Hyderabad
8	Mrs. VEERNALA SIREESHA	MRCEW Hyderabad
9	Mrs. POTNURU LAVNYA	MRCEW Hyderabad
10	Mrs. POLLELA JYOTHI	MRCEW Hyderabad
11	Mrs. NARMADA KARI	MRCEW Hyderabad
12	Mrs. MANJU PADIDELA	MRCEW Hyderabad
13	Mrs. CHINTALA KEERTHI	MRCEW Hyderabad
14	Mr. PITTA SANKARA RAO	MRCEW Hyderabad
15	Mrs. T. SUDHA	MRCEW Hyderabad
16	Mrs. P. GEETA SWARUPA	MRCEW Hyderabad

****

ISSN: 2229-3515

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief

Dr. C. SRINIVASA KUMAR
M. Tech., Ph. D
Professor
Dept. of Computer Science & Engineering
VIGNAN Institute of Technology & Management for Women, Hyderabad

Managing Editors

Mr. Sarma KSRK
Associate Professor
Vidhya Jyothi Institute of Technology
Hyderabad, Telangana, INDIA

Editorial Board

Dr. J. A. Chandulal Professor GITAM University, Visakhapatnam, AP	Dr. P. Rajendra Prasad Professor, Andhra University, Visakhapatnam, AP	Dr. M. Prabhakar Director, TRR Group of Institutions Hyderabad, AP, INDIA
Dr. A. Vinaya Babu Principal JNTU CEH JNTU, Hyderabad, AP	Dr. V. Sujatha Professor & Head, ChE Andhra University Visakhapatnam, AP,	Dr. D. Rajya Lakshmi Professor & Head Dept. of CSE JNTU Vijayanagaram, AP
Dr. V. Madhusudhan Rao Director, Engg.& Technology VIGNAN University, Vadlamudi, Guntur, AP	Dr. V. Kamakshi Prasad Professor Dept.of CSE JNTU Hyderabad, AP	Dr. K. Srinivasa Rao Principal TRR College of Engineering Hyderabad, AP, INDIA
Dr. M.N.Giri Prasad Professor, ECE JNTU Ananthapur, AP	Dr. D. Raghurami Reddy Dean Academics MRECW, Hyderabad, AP	Dr. Y. Radhika CSED, GITAM University, Visakhapatnam, AP, INDIA
Dr. L. Satya Prasad Principal Narasimha Reddy Engg.. College, Hyderabad, AP	Dr. Deepak Garg Professor, CSED Thapar University Patiala, Punjab, INDIA	Dr. M. V. Sathish Kumar Professor Tezpur University Tezpur, ASSAM, INDIA
Dr. P. V. Naganjaneyulu Principal P.N.C & Vijai Institute of Engg & Tech, Guntur, AP	Dr. N. Kishore Kumar Indian Institute of Technology, Gandhinagar Gujarat, INDIA	Dr. J. Pardha Saradhi Professor & Head,MBA RRS College of Engg & Tech. Hyderabad, AP, INDIA

Consulting Editor

Mr. Sarma KSRK Head, CSED Sreenivasa College of Engineering & Tech. Kurnool, AP, INDIA	Mr. M A Shiva Kumar Assistant Professor,CSED VIGNAN Institute of Technology & Sciences, Hyderabad

International Advisory Body

Mr. L. Narendra Kumar Glasgow Lankashire G20 7QE, UK	Dr.Ahmad J. Rusumdar Scientist, Karlsruhe Institute of Technology (KIT), IMVT, Germany	Dr. V. R. Chirumamilla Scientist, Eindhoven University of Tech., Eindhoven, North Brabant, Netherlands

Subscription

Price Per Volume (2 Issues): Rs. 2000(India), US $. 125(Foreign)

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

INTERNATIONAL JOURNAL OF ADVANCES IN SOFT COMPUTING TECHNOLOGY

Volume: 8 *Special Issue of NCSCCSS-2K18* *16 – 17th November, 2018*

* * * * * * *

A IMPERATIVE VICINITY RELIANT ROUTINE TO DECLINE QUERY LATENCY

Dr. K. Srujan Raju and Dr. M. Varaprasad Rao

Department of CSE, CMR Technical Campus, Kandlakoya (V), Medchal Road, Hyderabad – 501401, Telangana, India.
(✉ drksrujanraju@gmail.com)

ABSTRACT: Our IPRE plan and ˆss-tree can be utilized for searching records inside a given weighted Euclidean distance or great-circle distance too. Weighted Euclidean distance can be used to determine the significant difference in lots of types of data, while great-circle distance may be the distance of two points at first glance of the sphere. Benefits of suggested system: To the very best of our understanding, there doesn't exist predicate/predicate-only plan supporting inner range of products. Though our plan can be used for privacy preserving spatial range query within this paper, it might be used in other applications too. Experiments on the implementation show our option would be extremely powerful. To supply good user encounters, the POI search performing in the cloud side should be done very quickly The LBS provider isn't prepared to disclose its valuable LBS data towards the cloud. Many LBS users are mobile users, as well as their terminals are smart phones with limited sources. We advise EPLQ, a competent solution for privacy preserving spatial range query. Particularly, we reveal that whether a POI matches a spatial range query or otherwise can be tested on analyzing if the inner product of two vectors is within confirmed range. Within this paper, we concentrate on the latter setting. Within the former setting, there's an LBS provider holding a spatial database of POI records in plaintext, and LBS users query POIs in the provider's site. The LBS provider has abundant of LBS data that are POI records.

Keywords: Location-based services (LBS), outsourced encrypted data, privacy-enhancing technology, and spatial range query.

1. INTRODUCTION:

Spatial range totally a broadly used LBS, which enables a person to locate sights (POIs) inside a given distance to his/her location, i.e., the query point. While LBS are popular and vital, many of these services today including spatial range query require users to submit their locations, which raises serious concerns concerning the dripping and misusing of user location data. Protecting the privacy of user location in LBS has attracted considerable interest. However, significant challenges still stay in the style of privacy-preserving LBS, and new challenges arise particularly because of data outsourcing. Let's go ahead and take spatial range query, one type of LBS that we'll concentrate this paper, for example. However, the cryptographic or privacy-enhancing techniques accustomed to realize privacy-preserving query usually lead to high computational cost and/or storage cost at user side. Spatial range totally a web-based service, and LBS users are responsive to query latency [1]. To supply good user encounters, the POI search performing in the cloud side should be done very quickly. Again, the strategy accustomed to realize privacy-preserving query usually boost the search latency. We advise IPRE, which enables testing if the inner product of two vectors is at confirmed range without disclosing the vectors. In predicate file encryption, the important thing akin to a predicate f can decrypt a cipher text if and just when the attribute from the cipher text x satisfies the predicate. Though our plan can be used for privacy preserving spatial range query within this paper, it might be used in other applications too. Our techniques can be used as more types of privacy preserving queries over outsourced data. Within the spatial range query discussed within this work, we consider Euclidean distance that is broadly utilized in spatial databases. Weighted Euclidean distance can be used to determine the significant difference in lots of types of data, while great-circle distance may be the distance of two points at first glance of the sphere. Using great-circle distance rather of Euclidean distance for lengthy distances at first glance of earth is much more accurate. Within this paper, aiming at spatial range query, a well known LBS supplying details about sights (POIs) inside a given distance, we produce an efficient and privacy-preserving location-based query solution, known as EPLQ. Using the pervasiveness of smart phones, location based services (LBS) have obtained considerable attention and be popular and vital lately. To lessen query latency, we further design a privacy-preserving tree index structure in EPLQ. However, using LBS also poses a possible threat to user's location privacy. Particularly, to attain privacy preserving spatial range query, we advise the very first predicate-only file encryption plan for inner range of products (IPRE), that you can use to identify whether a situation is at confirmed circular area inside a privacy-preserving way.

The 2 vectors retain the location information from the POI and also the query, correspondingly. According to this discovery and our IPRE plan, spatial range query without dripping location information is possible. To prevent checking all POIs to locate matched POIs, we further exploit a singular index structure named ˆ ss-tree, which conceals sensitive location information with this IPRE plan.

2. CONVENTIONAL SCHEME:

Lately, we already have some solutions for privacy preserving spatial range query. Protecting the privacy of user location in LBS has attracted considerable interest. However, significant challenges still stay in the style of privacy-preserving LBS, and new challenges arise particularly because of data outsourcing. Recently, there's an increasing trend of outsourcing data including LBS data due to its financial and operational benefits. Laying in the intersection of traveling with a laptop and cloud-computing, designing privacy-preserving outsourced spatial range query faces the difficulties [2]. Disadvantages of existing system: Challenge on querying encrypted LBS data. The LBS provider isn't prepared to disclose its valuable LBS data towards the cloud. The LBS provider encrypts and outsources private LBS data towards the cloud, and LBS users query the encrypted data within the cloud. Consequently, querying encrypted LBS data without privacy breach is a huge challenge, and we have to safeguard not just the consumer locations in the LBS provider and cloud but additionally LBS data in the cloud. Challenge around the resource consumption in cellular devices. Many LBS users are mobile users, as well as their terminals are smart phones with limited sources. However, the cryptographic or privacy-enhancing techniques accustomed to realize privacy-preserving query usually lead to high computational cost and/or storage cost at user side. Challenge around the efficiency of POI searching. Spatial range totally a web-based service, and LBS users are responsive to query latency. Again, the strategy accustomed to realize privacy-preserving query usually boost the search latency. Challenge on security. LBS data have to do with POIs in real life. It's reasonable to visualize the attacker might have some understanding about original LBS data. With your understanding, known-sample attacks are possible.

3. ENHANCED METHOD:

Within this paper, we advise a competent solution for privacy-preserving spatial range query named EPLQ, which enables queries over encrypted LBS data without disclosing user locations towards the cloud or LBS provider. To safeguard the privacy of user location in EPLQ, we design a singular predicate-only file encryption plan for inner range of products, which, to the very best of our understanding, may be the first predicate/predicate-only plan of the kind. To enhance the performance, we design a privacy preserving index structure named ˆss-tree. Particularly, the primary contributions of the paper are three folds. We advise IPRE, which enables testing if the inner product of two vectors is at confirmed range without disclosing the vectors. In predicate file encryption, the important thing akin to a predicate f can decrypt a cipher text if and just when the attribute from the ciphertextx satisfies the predicate, i.e., f(x) = 1. Predicate-only file encryption is really a special kind of predicate file encryption not created for encrypting/decrypting messages. Rather, it reveals that whether f(x) = 1 or otherwise. Predicate-only file encryption schemes supporting various kinds of predicates happen to be suggested for privacy-preserving query on outsourced data [3]. The 2 vectors retain the location information from the POI and also the query, correspondingly. According to this discovery and our IPRE plan, spatial range query without dripping location information is possible. To prevent checking all POIs to locate matched POIs, we further exploit a singular index structure named ˆss-tree, which conceals sensitive location information with this IPRE plan. Our techniques can be used as more types of privacy preserving queries over outsourced data. Within the spatial range query discussed within this work, we consider Euclidean distance that is broadly utilized in spatial databases. Furthermore, security analysis implies that EPLQ is safe under known-sample attacks and cipher text-only attacks. Using great-circle distance rather of Euclidean distance for lengthy distances at first glance of earth is much more accurate. Particularly, for any mobile LBS user utilizing an Android phone, around .9 s is required to produce a query, and in addition it only needs a commodity workstation, which plays the function from the cloud within our experiments, a couple of seconds to look POIs. Additionally, extensive experiments are conducted, and also the results show EPLQ is extremely efficient in privacy preserving spatial range query over outsourced encrypted data.

System Framework: Privacy-preserving POI query continues to be studied in 2 settings of LBS: public LBS and outsourced LBS. The LBS provider enables approved users to make use of its data through location-based queries. LBS users possess the information that belongs to them locations, and query the encrypted records of nearby POIs within the cloud [4]. Cryptographic or privacy-enhancing techniques are often employed to hide the place information within the queries delivered to the cloud. To decrypt the encrypted records caused by the cloud, LBS users need to get the understanding key in the LBS provider ahead of time. The cloud has wealthy storage and computing sources. It stores the encrypted LBS data in the LBS provider, and offers query services for LBS users. Generally, within the outsourced LBS setting, the cloud can watch both queries from LBS users and encrypted LBS data in the LBS provider, which happens to be an benefit to learn user locations. Within this paper, we've suggested EPLQ, a competent privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. Two potential usages are privacy-preserving similarity query and lengthy spatial range query [5]. Therefore, presuming different abilities from the attacker, you will find mainly four attack models in outsourced LBS setting. That's, the cloud would honestly store and check data as requested however, the cloud would also provide financial incentives to understand individuals stored LBS data and user location data in query. Underneath the outsourced LBS system model, our design goal would be to develop a competent, accurate, and secure solution for privacy-preserving spatial range query. Though susceptible to more effective attacks for example known plaintext attacks, the answer suggested within this paper still may be used in lots of situations in which the attackers don't have the needed abilities or understanding.

Implementation: So, we use attribute vectors and predicate vectors to consult the attributes and predicates in IPRE. IPRE plan is really a symmetric predicate-only file encryption plan, also it includes four algorithms: Setup formula for establishing a public parameter PP, a characteristic file encryption key AK, along with a predicate file encryption key PK Enc formula for encrypting attribute vectors to cipher texts Gent ken formula for encrypting predicate vectors to tokens and appearance formula for checking if your cipher text's attribute satisfies a token's predicate. Before describing IPRE's algorithms, we define the encodings of attribute vectors and predicate vectors, which function as a foundation of IPRE. The formula of encrypting attribute vectors is really a probabilistic formula that takes a characteristic vector. The setup formula is really a probabilistic formula, that takes a burglar parameter ?, the attribute/predicate vector length t, as well as an inner range of products [t1, t2] as input. The ˆ ss-tree introduced within this jobs is a variant of ss-tree. For indexing spatial data, there really exist a number of data structures for example r-tree and ss-tree, and a number of them can be used as spatial range query. When such type of data structures can be used for privacy preserving query, location data [6]. Hence, we decide ss-tree because of its simplicity, and proposeˆ ss-tree according to ss-tree and IPRE. Poor spatial database of Cartesian coordinate system, the centroid is a set of coordinates (x, y). A leaf node's centroid may be the corresponding POI's coordinates, and it is radius is . A non leaf node's centroid and radius rely on its children. Its centroid may be the mean of its children's centroids. Its radius isn't smaller sized compared to distance between its centroid and then any descendant node's centroid. A node of ss-tree also offers another fields to aid tree building, approximation search, and sampling operations. We omit these fields within this paper because they are not highly relevant to our solution. Using the ss-tree, searching POI records matching a spatial range totally extremely powerful. Realizing that descendant nodes of the no leaf node have been in the no leaf node's connected circular area. Search POI records can be achieved by checking the ss-tree from root to leaves. ˆ ss-tree may be the core in our EPLQ solution. It's a variant of ss-tree. ˆ ss-tree hides each tree node's location information using our predicate-only file encryption plan, and removes unnecessary information. Due to the file encryption, discovering circular area intersection and matched records will also be different when searching matched records using the tree. Suppose a spatial range query really wants to find all POIs inside a circular area centered at coordinates (xi, yi) with radius ri. Because of the above tokens connected using the query, POI records matching the query are available by searching ˆ sstree. Looking starts in the root node. If your no leaf node's area intersects using the query area, all kids of the node is going to be scanned. Otherwise, all descendant nodes of the no leaf node are skipped.

Discovering circular area intersection and matched records derive from our IPRE plan for inner range of products [7]. To understand EPLQ, we've designed an IPRE along with a novel privacy-preserving index tree named ˆ ss-tree. EPLQ's effectiveness continues to be evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and cipher text-only attacks. The conventional file encryption plan accounts for stopping the cloud from learning POI records, while our IPRE plan accounts for protecting user location and POI location in the cloud. The present AES standard can be used the conventional plan, which is secure under cipher text-only, known-sample, and known-plaintext attacks.

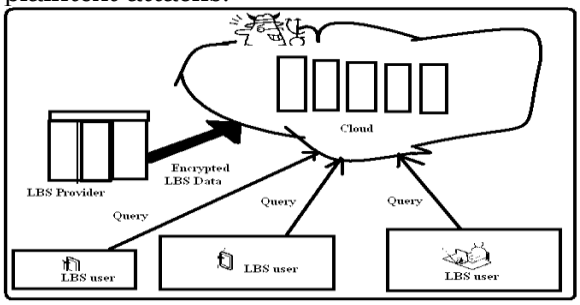


Fig.1.System architecture

4. CONCLUSION:

The suggested IPRE plan enables computing inner products and evaluating their values having a predefined range inside a privacy-preserving way. So far as we all know, our plan may be the first predicate/predicate-only file encryption plan for inner range of products. In IPRE, both attributes and predicates are vectors. The confidentiality of LBS data includes not just the confidentiality of POI records but the confidentiality of location information in ˆ ss-tree. The safety of EPLQ solution depends upon the actual standard file encryption plan and IPRE plan. By supporting these 2 kinds of distances, privacy-preserving similarity query and lengthy spatial range query may also be recognized. Detailed security analysis confirms the safety qualities of EPLQ.

REFERENCES:

[1] Lichun Li, Rongxing Lu, Senior Member, IEEE, and Cheng Huang, "EPLQ: Efficient Privacy-Preserving Location-BasedQuery Over Outsourced Encrypted Data", ieee internet of things journal, vol. 3, no. 2, april 2016.

[2] G. Ars, J.-C. Faugere, H. Imai, M. Kawazoe, andM. Sugita, "Comparison between XL and Gröbner basis algorithms," in Proc. ASIACRYPT, 2004, pp. 338–353.

[3] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Int. Conf. Perv. Serv. (ICPS), 2005, pp. 88–97.

[4] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, "Secure k-nearest neighbor query over encrypted data in outsourced environments," in Proc. IEEE 30th Int. Conf. Data Eng. (ICDE), 2014, pp. 664–675.

[5] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. 1st Int. Conf. Mobile Syst. Appl. Serv., 2003, pp. 31–42.

[6] E. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc. IEEE Symp. Secur. & Privacy, 2007, pp. 350–364.

[7] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

A RANDOMIZED VISUAL-SPLITTER FOR HUGE ENCRYPTED IMAGE

Dr.C.Jayaprakash[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 (✉ dr.jayaprakash.cs@gmail.com)

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

ABSTRACT: ***We advise a brand new protocol for secure multiplication between two parties, the aim of that is that every party obtains an arbitrary share from the product of the private inputs. While experiencing the abundant storage and computation sources for cost saving and versatility, the outsourcing of information storage and computation towards the cloud also raises great privacy and security concerns because of the different trust domains the information owner. we'll give a theoretical study of the potency of our plan step-by-step meaning the extracted features are not far from the outputs generated through the original SIFT. the expose of original image data towards the semi-reliable cloud company may inevitably reveal the information owner's personal data, like the personal identity, locations or perhaps financial profiles etc. Privacy-preserving outsourcing of image feature extraction provides the commitment of acquiring feature descriptors determined by personal information without exposing the information owner's privacy, while experiencing the abundant cloud computation sources. A number of orientations will be designated to every key point in line with the local image gradient direction. Because of the need for image feature extraction in multimedia information systems and it is heavy operations on massive data, specifically for satellite data because of its tremendous size and many feature points, the extraction or recognition of image features in the ciphertext domain has started to draw in increasingly more research interest. The extracted feature vectors done by outsourced SIFT formula should bond with the outcomes from original SIFT formula whenever possible. Our experimental results reveal that our protocol outperforms the condition-of-the-art and performs comparably towards the original SIFT and it is simple for real-world applications.***

Keywords: Privacy preserving, security, homomorphic encryption, cloud computing scale-invariant feature transform.

1. INTRODUCTION:

Within this paper, we advise a highly effective and practical privacy-preserving computation outsourcing protocol for that prevailing scale-invariant feature transform (SIFT) over massive encrypted image data. While putting great effort around the privacy or efficiency aspect, one common limitation from the previous solutions is they all lack comprehensive analysis and evaluations with regards to the upkeep from the key characteristics from the original image feature extraction formula [1]. We assume S1 and S2 are independent with one another and could be thought to fit in with two independent cloud providers like Amazon . com EC2 and Microsoft Azure. Within this work, we presented a brand new and novel privacy-preserving SIFT outsourcing protocol according to recently suggested secure interactive protocols BSMP and BSCP. Both of us carefully evaluate and extensively assess the security and effectiveness in our design. To safeguard the privacy, O will first secure each image set after which distribute the ciphertexts to S1 and S2. Hence, it's important to possess a minimum of two independent entities for achieving privacy-preserving image feature extraction outsourcing. In computer vision and pattern recognition, scale-invariant feature transform (SIFT) is a vital feature extraction formula that's been broadly used because of its distinctiveness and powerful matching across a considerable selection of affine distortion, inclusion of noise, and alter in illumination. Homomorphic file encryption is really a public-key file encryption plan that supports significant operations within the encrypted data. Particularly, somewhat homomorphic file encryption (SHE) is really a plan that allows a restricted quantity of both addition and multiplication operations around the ciphertexts. A match between your interest point and it is nearest point occurs when the distance ratio between both of these points is below a threshold t. We conduct experiments on real image dataset: INRIA Graffiti, containing pictures of graffiti-covered walls obtained from different camera viewpoints changes [2].

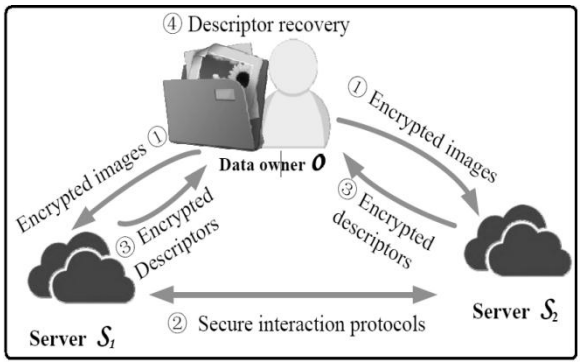


Fig.1.Proposed system framework

2. METHODOLOGY:

Regardless of the tremendous benefits, the outsourced multimedia data and it is originated applications may reveal the information owner's personal data, like the personal identity, locations or perhaps financial profiles. This observation has lately turned on new information interest on privacy-preserving computations over outsourced multimedia data [3]. Within the existing literature, efforts on privacy-preserving outsourcing computation happen to be dedicated to various mathematical problems including modular exponentiation, straight line equations and kNN search. We evaluate our protocol comprehensively with real life massive image datasets. By leveraging the above mentioned two qualities, all of the operations of original SIFT, including common addition, multiplication and comparison, can be achieved over ciphertexts. Ideas also think that the entire quantity of integers N is really a multiple from the batched number 1 for easy representation as did in BSMP. Then S2 will compute the above mentioned equations over ciphertexts in line with the homomorphic qualities. However, a cautious of the solution implies that their plan has two primary limitations making it inapplicable to real-world applications as first stated. Probably the most appealing benefits of SHE would be that the batching technique: single-instruction multiple-data (SIMD) of may be used to lessen the communication cost and accelerate the computation on ciphertexts when solving problems on the massive. S1 and S2 operate a key point localization protocol according to BSCP to obtain the candidate key point locations without compromising the privacy that belongs to them inputs. They will eliminate edge responses to acquire stable key points using BSMP. Finally, the locations are revealed towards the two servers. For any detected candidate key point D1(x y z) around the server S1, its derivatives in x-direction, y-direction and xy-direction are first computed the following to constitute its Hessian matrix. As the amount of the key points varies using the images' content, the typical quantity of key points cannot provide a better illustration and therefore we simply choose three specific images with size 3000 X 3000 for highly structured image, poorly structured image and texture image. the servers are only able to acquire some inequalities concerning the pixel values, so they need to traverse all of the options for every pixel that satisfy these inequalities. We reason that to be able to rebuild the entire image, probably the most helpful details are the understanding from the relationship between any two neighboring pixels while other inequality constraints have limited contribution in recovering pixels [4]. The cloud servers will work cooperatively to accomplish the k-nn search task and return a precise Google listing without acquiring anything private concerning the descriptors. This process could be directly coupled with our plan so that the information owner can relieve them self in the burden of computationally-intensive search jobs. The 2 recently suggested protocols are made according to SHE integrated with SIMD that are proven to outshine the present methods in efficiency when it comes to both computation and communication overhead [5]. To lessen the models of interactions within the implementation of BSCP and BSMP, S1 can prepare all of the data concurrently and transmit all of the encrypted data inside a onetime transmission. While finding peaks, our goal is to find out which is bigger between two bins within the original histogram H. we assess the time cost and also the communication price of our plan around the server side. Observe that the servers and also the data owner are simulated on machines of the identical configuration without needing multithreading or other parallel techniques. However, we reveal that there is exponential quantity of possible reconstructions that fulfill the given constraints between any two neighboring pixels [6].

3. BSMP AND BSCP:

The authors contended the locations of key points are safe from revealing towards the cloud. However, we reveal that this isn't true also it violates their security statements. Both of us carefully evaluate and extensively assess

the security and effectiveness in our design. We design two novel secure interactive protocols BSMP and BSCP which allow the 2 servers to compute these products making comparisons of multiple pairs of integers concurrently with privacy upkeep by utilizing somewhat homomorphic file encryption (SHE) and also the batching technique SIMD.

4. CONCLUSION:

We'll theoretically reveal that the approximate orientation substitution within the image rotation includes a really low error probability, which may be overlooked. Within the orientation assignment, each direction is situated in an interval, so we make use of the median to represent its value. Consequently, for locations with multiple peaks of comparable magnitudes, there is multiple tips produced at same position and scale, however with different orientations because the original SIFT does. Observe that, within the above protocol, constant-round interactions may also be achieved by encrypting all of the data concurrently and transmitting the encrypted data previously.

REFERENCES:

[1] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel and Distributed Systems, 2015, DOI: 10.1109/TPDS.2015.2506573.

[2] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 10, pp. 1615–1630, 2005.

[3] F. Perronnin, J. S´anchez, and T. Mensink, "Improving the fisher kernel for large-scale image classification," in Proc. of ECCV'10. Springer, 2010, pp. 143–156.

[4] M. Schneider and T. Schneider, "Notes on non-interactive secure comparison in image feature extraction in the encrypted domain with privacy-preserving sift," in Proc. of IH & MMSec'14. ACM, 2014, pp. 135–140.

[5] Q. Wang, S. Hu, K. Ren, J. Wang, Z. Wang, and M. Du, "Catch me in the dark: Effective privacy-preserving outsourcing of feature extractions over image data," in Proc. of INFOCOM'16, Accepted to appear, 2016.

[6] L. Weng, L. Amsaleg, A. Morton, "A privacy-preserving framework for large-scale content-based information retrieval," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 15

A SIMPLE WAY OF DOCUMENTATION FOR UNEXPECTED BEHAVIOR OF COMPONENTS

Mr. G. Prabhakar Reddy., Mrs. K. Archana

Assistant Professor, Department of CSE., Malla Reddy Institute of Engineering & Technology., Maisammaguda., Medchal., TS, India

(✉ prabhakar.sp17@gmail.com)

ABSTRACT: ***The ranking function is understood to be a weighted mixture of features, in which the features draw heavily on understanding specific towards the software engineering domain to be able to measure relevant relationships between your bug report and also the source code file. The primary contributions of the paper include: a ranking method of the issue of mapping source files to bug reports that allows the seamless integration of the wide diversity of features exploiting formerly fixed bug reports as training examples for that suggested ranking model along with a learning-to-rank technique while using file dependency graph to define features that capture a stride of code complexity. This paper introduces an adaptive ranking approach that leverages project understanding through functional decomposition of source code, API descriptions of library components, the bug-fixing history, the code change history, and also the file dependency graph. The suggested adaptive ranking approach is usually relevant to software projects that there is an adequate amount of project specific understanding, like a comprehensive API documentation. Given an insect report, the ranking score of every source file is computed like a weighted mixture of a range of features, in which the weights are trained instantly on formerly solved bug reports utilizing a learning-to-rank technique. We assess the ranking system on six massive free Java projects, while using before-fix form of the work for each bug report.***

Keywords: Ranking model, Bug reports, software maintenance, learning to rank, API, adaptive ranking.

1. INTRODUCTION:

An insect report provides information which may help in fixing an insect, using the overall purpose of increasing the software quality. A developer who's assigned an insect report usually must reproduce the abnormal behavior and perform code reviews to find the reason [1]. Whenever a new bug report is received, developers usually have to reproduce the bug and perform code reviews to obtain the cause, a procedure that may be tiresome and time intensive. Consequently, we make use of the change good reputation for source code like a strong signal for linking fault-prone files with bug reports. We predict complex code to become more vulnerable to bugs than simple code. Experimental results around the before-fix versions reveal that our bodies considerably outperform numerous strong baselines in addition to three recent condition-of-the-art approaches. Something for ranking the entire source files regarding how likely they're to contain the reason for the bug would enable developers to narrow lower their search and improve productivity. In addition, the ranking performance can usually benefit from informative bug reports and extensively recorded code resulting in a much better lexical similarity. We hypothesize that both kinds of features are helpful when put together as a general ranking model. Compound words for example “Work Bench” are split up into their components according to capital letters, although modern-day methods [2]. However, we are able to bridge the lexical gap using the API specs from the classes and interfaces utilized in the origin code. Our hypothesis would be that the signal becomes more powerful once the class name is longer and therefore more specific. Because the inner product utilized in the cosine similarity function has non-zero terms just for tokens which are in keeping between your bug report and also the source file. In addition, the suggested ranking model outperforms three recent condition-of-the-art approaches. Feature evaluation experiments employing greedy backward feature elimination show all features are helpful. An associated problem can happen once the bug report is extremely similar having a particular kind of content from the source file and different with anything else, the cosine similarity using the entire file is extremely small because of its large size. The report-based bug localization approach computes a general ranking score because the simple amount of the lexical similarities of possible eight document-query field pairs. A precise way of measuring code complexity will need a great representation from the semantics from the code. To produce the file dependency graph, we extract the file dependency relationships of all Java files

inside a project while using Eclipse JDT AST Parser. An internet page having a high hub score is known as a great listing of links to a lot of authority pages. Later on work, we'll leverage additional kinds of domain understanding, like the stack traces posted with bug reports and also the file change history, in addition to features formerly utilized in defect conjecture systems [3].

2. TRADITIONAL APPROACH:

Lately, scientific study has developed methods that focus on ranking source files for given bug reports instantly. Sahaet al. syntactically parses the origin code into four document fields: class, method, variable, and comment. The summary and also the description of the bug report are thought as two query fields. Kim et al. propose both a 1-phase along with a two-phase conjecture model to recommend files to repair. Within the one-phase model, they've created features from textual information and metadata of bug reports, apply Naive Bayes to coach the model using formerly fixed files as classification labels, after which make use of the trained model to assign multiple source files to some bug report. Rao and Kak apply various IR models to determine the textual similarity between your bug reports along with a fragment of the source file [4]. Disadvantages of existing system: Their one-phase model uses only formerly fixed files as labels within the training process, and for that reason cannot be employed to recommend files that haven't been fixed before when being presented with a brand new bug report. Existing methods require runtime executions.

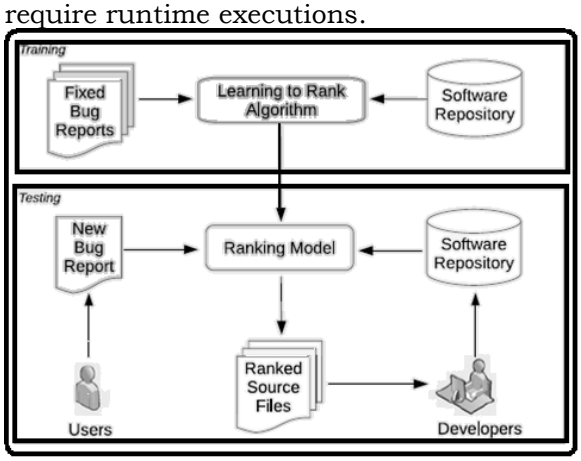


Fig.1.Framework of Bug Report

3. BUG REPORT METHOD:

To discover a bug, developers use not just the information from the bug report but additionally domain understanding highly relevant to the program project. while using file dependency graph to define features that capture a stride of code complexity fine-grained benchmark datasets produced by looking into a before-fix form of the origin code package for every bug report extensive evaluation and comparisons with existing condition-of-the-art methods along with a thorough look at the outcome that has dress in the ranking precision. Benefits of suggested system: Our approach can locate the appropriate files inside the top ten strategies for over 70 % from the bug reports in Eclipse Platform and Tomcat. In addition, the suggested ranking model outperforms three recent condition-of-the-art approaches. Feature evaluation experiments employing greedy backward feature elimination show all features are helpful.

Fine-grained Datasets: Another buggy file may not even appear in the fixed revision, whether it was deleted following the bug was reported. However, software bugs are frequently present in different revisions from the source code package [5]. To prevent the issues connected with utilizing a fixed code revision, we produce a fine-grained benchmark dataset for every project by looking into a before-fix form of its source code package for each bug report. Therefore, for every bug report, the form of the related software program before the fix was committed was utilized within the experiment. To map an insect report using its fixed files, we use the heuristics suggested by Dallmeier and Zimmermann. For just about any given bug report r, the machine ranking is produced by computing the weighted scoring function, for every source code file s within the project, adopted by ranking all of the files in climbing down order of the scores.

Rank Implementation: Within this approach, learning w is equivalent with solving the optimization problem. The purpose of this formulation is to locate a weight vector w so that the related scoring function ranks the files that are recognized to be relevant for any bug report towards the top of their email list for your bug report. The entire number N of possible training triplets is not directly based on the amount of bug reports selected to become incorporated in R, the amount of relevant files. To maximize their utility, you want to select irrelevant files that are the same bug report. Therefore, we first make use of the VSM cosine similarity feature, to position all of the files within the project after which select just the top irrelevant files for training [6]. We used Spearman's rank correlation to look for the similarity between your sources file

rankings akin to consecutive points. The greater recent bug reports are anticipated to higher match the qualities from the bugs in the present testing fold, which is anticipated to guide to optimal weights within the ranking function. As the evaluation results acquired on this type of dataset may be used to compare different methods to file ranking for bug reports, the particular performance figures. The textual similarity between your bug report and also the source code file will be computed individually for every field type. We introduced a learning-to-rank approach that emulates the bug finding process utilized by developers. The ranking model characterizes helpful relationships from a bug report and source code files by leveraging domain understanding, for example API specifications, the syntactic structure of code, or issue tracking data. Even though the primary reason for our work is a technique for mapping bug reports to relevant source code files, within this section we describe and evaluate an easy adaptation in our learning-to-rank system that allows it to carry out a finer-grained ranking, at the amount of methods. We match it up simple adaptation in our system using the condition-of-the-art feature location approach. Our model doesn't use execution traces and for that reason doesn't need to reproduce the bug. However, we use features produced from the file revision history, an origin of evidence that isn't used. Our utilization of greedy backward elimination is motivated by research showing that wrapper methods be more effective at producing features sets that suit the training formula. After ranking the origin code files, the following two stages in the formula rank the techniques within each file and remove methods whose similarity using the bug reports falls below a predefined threshold [7].

4. CONCLUSION:

Our model doesn't use execution traces and for that reason doesn't need to reproduce the bug. However, we use features produced from the file revision history, an origin of evidence that isn't used. When along with runtime analysis, the feature evaluation results may be used to pick a subset of features to have a target trade-off between system precision and runtime complexity. The primary contributions of the paper include: a ranking method of the issue of mapping source files to bug reports that allows the seamless integration of the wide diversity of features exploiting formerly fixed bug reports as training examples for that suggested ranking model along with a learning-to-rank technique We introduced a learning-to-rank approach that emulates the bug finding process utilized by developers. To maximize their utility, you want to select irrelevant files that are the same bug report. Therefore, we first make use of the VSM cosine similarity feature, to position all of the files within the project after which select just the top irrelevant files for training. Experimental evaluations on six Java projects reveal that our approach can locate the appropriate files inside the top ten strategies for over 70 % from the bug reports in Eclipse Platform and Tomcat.

REFERENCES:

[1] Xin Ye, Student Member, IEEE, RazvanBunescu, and Chang Liu, Senior Member, IEEE, “Mapping Bug Reports to Relevant Files:A Ranking Model, a Fine-Grained Benchmark,and Feature Evaluation”, ieee transactions on software engineering, vol. 42, no. 4, april 2016.

[2] T. Joachims, “Optimizing search engines using clickthrough data,” in Proc. 8th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, New York, NY, USA, 2002 pp. 133–142.

[3] S. K. Bajracharya, J. Ossher, and C. V. Lopes, “Leveraging usage similarity for effective retrieval of examples in code repositories,” in Proc. 18th ACM SIGSOFT Int. Symp. Found. Softw. Eng., New York, NY, USA, 2010 pp. 157–166.

[4] S. Breu, R. Premraj, J. Sillito, and T. Zimmermann, “Information needs in bug reports: Improving cooperation between developers and users,” in Proc. ACM Conf. Comput. Supported Cooperative Work, New York, NY, USA, 2010, pp. 301–310.

[5] T. Dasgupta, M. Grechanik, E. Moritz, B. Dit, and D. Poshyvanyk, “Enhancing software traceability by automatically expanding corpora with relevant documentation,” in Proc. IEEE Int. Conf. Softw. Maintenance, Washington, DC, USA, 2013, pp. 320–329.

[6] A. Marcus, A. Sergeyev, V. Rajlich, and J. I. Maletic, “An information retrieval approach to concept location in source code,” in Proc. 11th Working Conf. Reverse Eng., Washington, DC, USA, 2004,pp. 214–223.

[7] A. T. Nguyen, T. T. Nguyen, J. Al-Kofahi, H. V. Nguyen, and T. N. Nguyen, “A topic-based approach for narrowing the search space of buggy files from a bug report,” in Proc. 26th IEEE/ACM Int. Conf. Autom. Softw. Eng., Washington, DC, USA, 2011 pp. 263–272.

A TIME-BOUND UPLOADING USING LESS-COST FRAMEWORK

Dr.A.Janardhan* and Dr. J. Nelson

Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ dhana48@yahoo.co.in)

ABSTRACT: ***Recently, extensive research efforts happen to be dedicated to data gathering in WSNs. Many of them centered on static data gathering where sensing information is collected with a static sink. The practicality of utilizing multiple-input-multiple-output (MIMO) in WSNs to lessen data transmission some time and improve spatial diversities continues to be studied within the literature. Upon finding the initial issue is non-convex, we morph it into a convex one by presenting auxiliary variables and logarithmic transformation. Our statistical results demonstrate that the suggested algorithms can converge best within 50 iterations. We conduct extensive simulations to exhibit our framework can considerably reduce data gathering some time and total energy consumption when compared to algorithms without concurrent data uploading and power control. For low power devices for example sensors, interference is generally small therefore we would expect straight line decorrelator to possess comparable performance with MMSE receiver. The primal and dual problems have optimal solutions. Thus, it may be efficiently tackled by convex programming techniques. We make use of the Lagrangian dual decomposition to split up correlated variables. When a sensor node detects that it is funnel towards the SenCar is idle, it adaptively distributes its data total subcarriers by selecting appropriate constellations according to funnel conditions on every subcarrier, and transmits the information over different subcarriers. We realize that the congestion cost yij and also the sojourn time bound T determine the sojourn duration of the SenCar at anchor point a. Lagrangian multiplier $a could be known as the cost of sojourn time allocation at anchor point a, which depends upon the entire sojourn time bound***

Keywords: Wireless sensor, data gathering cost, convex optimization, elastic link capacity, distributed algorithms, Lagrangian multiplier.

1. INTRODUCTION:

Within this paper we advise a brand new data gathering cost minimization framework for mobile data gathering in wireless sensor systems by thinking about dynamic wireless link capacity and power control jointly. Our new framework not just enables concurrent data uploading from sensors towards the mobile collector, but additionally determines transmission power under elastic link capacities. presenting MIMO communications incurs more overhead within the system [1]. However, because the SenCar could be outfitted having a high-density battery power with plenty of energy and has the capacity to perform more complicated computations than sensor nodes, we concentrate on the overhead in the sensor's side. the immediate fa ij might be influenced by interference or congestions while transmissions are now being initiated. However, for a longer period, the traffic flow would achieve stability when physical and MAC layer protocols have been in effect. For sensors, they consume energy to deliver packets. For that SenCar, it consumes energy to maneuver, collect, decode collected packets and process sensing data. Our work aims to reduce the entire data gathering cost by dynamically modifying the information rates, link flows and SenCar's sojourn time restricted by some constraints. To lessen redundancy because of data correlation, we use a distributed spatial coding technique known as Slepian-Wolf coding introduced.

In the Slopian-Wolf theorem, we all know that nodes can jointly encode their data individually for a price lower-bounded by their joint entropy as lengthy because the Slepian-Wolf constraint is content. A layer includes a number of sub problems. Functions of primal or Lagrangian dual variables supply the interfaces between different layers. The aim of PCSA would be to provide a distributed protocol for optimal power allocation within the physical layer.

The aim for power control would be to ensure two sensors to become compatible while figuring out appropriate link capacities [2]. The transmission range and interference range vary using the transmission power and also the funnel status.

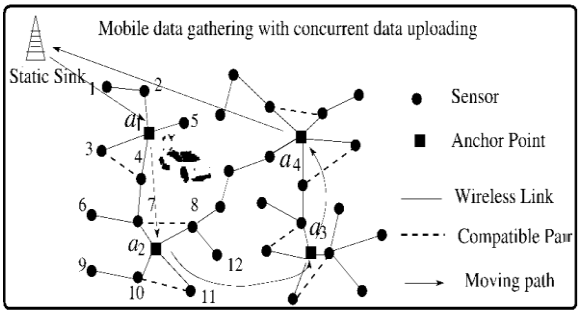


Fig.1.Proposed framework

2. METHODOLOGY:

Within this paper, we've developed a mix-layer optimization framework for mobile data gathering in WSNs thinking about elastic link capacity and power control on sensors. Pazzi and Boukerche suggested a mobile data collecting technique for delay-sensitive applications to ease high traffic load and bottleneck inside a sink's vicinity. Throughout the operation, sensors organize themselves right into a network and report sensing data towards the sink(s) periodically [3]. To conform with MIMO communication paradigm, you should ensure the amount of concurrent data traffic flows is a maximum of the amount of antennas. Because the SenCar is outfitted with two antennas, for the most part two sensors are permitted to concurrently transmit data. In WSNs, because of the overlap of sensing ranges, data might be redundant or correlated. Transmitting redundant data within the network consumes unnecessary energy and reduces throughput from the network. Hence, it's desirable to lessen redundancy. The expression could be described as that data generated at sensors near to one another might have some correlations [4]. Once we boost the distance, there's little correlation given distinct geographical occasions observed by sensors which correlation tremendously declines on distance. Observe that the transmission power affects not just the SINR but the communication range despite a non-deterministic propagation funnel because the received signal power attenuates tremendously using the transmission distance because of path loss, shadowing and multipath. A method to remove this inters ream interference from your interested sensor would be to project the received signal y to the subspace orthogonal towards the one spanned through the other funnel vector. Any two sensors i and m that satisfy these criteria can effectively make concurrent data uploading towards the SenCar. This type of sensor pair is called a compatible pair. There's two explanations why a sensor node splits its data to upload to various anchor points, rather of simply selecting probably the most energy-efficient anchor indicate upload all of the data [5]. We make use of the sub gradient formula in line with the dual decomposition method, which is an excellent way of convex programs and may naturally achieve distributed implementation. The greater available buffer space a sensor has, the bigger distinction between outgoing and incoming rates, which means a decreasing cost and much more data the sensor can generate. we advise a competent search formula in line with the KKT conditions to locate an ideal solution. Without effort, when the local queuing delay is big or even the congestion is heavy for any sensor, its transmission power should increase or increase moderately when the current electricity has already been high. If queuing delays on other links are lengthy, the transmission power this sensor ought to be decreased to be able to lessen the interference on individual's links. by presenting auxiliary variables, we transform the non-convex problem right into a convex one and additional decompose it into several sub problems of information control and knowledge split in the transport layer, routing in the network layer, and power control and compatibility decisions in the physical layer. Power control in the physical layer cooperates with data routing in the network layer to update sensors' routing strategies and power allocation [6]. When compared with Fixed-Rate, both DaGCM and Shortest-Path have lower energy consumption. Such inclination gets to be more distinct using the increase of the amount of sensors that is related to the critical role that power control plays in lessening energy consumption. We first compare the performance between DaGCM formula and also the prices-based formula when it comes to total data gathering some time and total energy consumption, to show the benefits of concurrent data uploading and power control. The updates reveal that for sensor i to look for the data amount submitted towards the SenCar at anchor point a, the information generating cost message ought to be transferred in the data control sub algorithm towards the data split sub algorithm.

3. BALANCING TRAFFIC LOAD:

To obtain additional flexible data gathering tours for mobile collectors, Ma and Yang suggested an formula for planning the moving road to mobile collectors and balancing traffic load in multi-hop systems. We employ the sub gradient iteration formula to resolve the minimization problem. We first relax the issue with Lagrangian idealization, then decompose the initial problem into several sub problems, and offer distributed algorithms to derive data rate, link flow and routing, power control, and transmission compatibility. The outcomes reveal 20 % shorter data collection latency

typically with lower energy consumptions when compared with previous works in addition to lower data gathering cost and sturdiness in situation of node failures. For MMSE receiver, a matrix inversion with how big filter inputs is required to obtain optimal tap weights. This operation can lead to greater complexity, typically around the order of N2 to N3 operations, where N is the amount of filter inputs.

4. CONCLUSION:

The information control sub algorithm aims to look for the optimal quantity of data generated each and every sensor by solving DP1. We further explore the performance comparison between DaGCM formula along with other mobile data gathering strategies. Meanwhile, we realize that when compared with other two algorithms, DaGCM formula pays the cheapest cost for collecting the equivalent data. With regard to fairness, the flow rate each sensor uses in Fixed-Rates are the allowable maximum rate that may avoid traffic jam within the network. Because the SenCar has effective transceivers and-density batteries, it may perform computations to allocate the perfect sojourn time ta each and every anchor point.

REFERENCES:

[1] C. Long, B. Li, Q. Zhang, B. Zhao, B. Yang, "The endto-end rate control in multiple hop wireless networks: Cross-layer formulation and optimal allocation," IEEE J. Sel. Areas Commun., v26/4, pp.719–731, 2008.

[2] G. Hanif and D. Sherali, "Recovery of primal solutions when using subgradient optimization methods to solve lagrangian duals of linear programs," Oper. Res. Lett., vol. 19, no. 3, pp. 105–113, 1996.

[3] M. Chiang, "Balancing transport and physical layers in wireless multihop networks: Jointly optimal congestion control and power control," IEEE J. Sel. Areas Commun., vol. 23, no. 1, pp. 104–116, Jan. 2005.

[4] M. Gatzianas and L. Georgiadis, "A distributed algorithm for maximum lifetime routing in sensor networks with mobile sink," IEEE Trans. Wireless Commun., vol. 7, no. 3, pp. 984–994, Mar. 2008.

[5] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," IEEE J. Sel. Areas Commun., vol. 22, no. 6, pp. 1089–1098, Aug. 2004.

[6] M. Zhao and Y. Yang, "Optimization based distributed algorithm for mobile data gathering in wireless sensor networks," IEEE. Trans. Mobile Comput., vol. 11, no. 10, pp. 1464–1477, Oct. 2012.

A USER-CENTRIC TECNHNIQUE BASED ON CURRENT SUBSTANTIAL REGION IN PASS THROUGH

Tulasi Nadh, V* and M. Kranthi Reddy

Assistant Professor, Department of CSE., Vignan Institute of Technology and Science, Deshmukhi, Hyderabad, TS, India (✉ tulasinadhv@gmail.com)

.

ABSTRACT: ***The provenance of location is an important requirement in path critical scenarios. A legitimate claim of travel path must be verified with regards to the location provenance. Continuous tracking of users by providers including third-party applications violates the users' privacy, enables traceable identities, and helps make the users defenseless against untrusted providers. Any two-entity based location proof protocol has four different collusion combinations. A 2-party protocol may have a minimum of one combination that the system is going to be susceptible to, where both parties are malicious. We've presented the WORAL framework implementation an entire ready-to-deploy suite of applications, supporting Android based devices to gather and export location proofs, including wearable add-ons, for example Google Glass. The place authority or even the user can produce a puppet witness to create false asserted proofs or relay the assertion demands to some remote witness who isn't co-found at the given site during the time of visit. Within the WORAL framework, users, witnesses, LAs, and auditors have to on line using the SP utilizing a unique identification criteria. Within this paper, we introduce WORAL, a ready to-deploy framework for secure, witness-oriented, and provenance preserving location proofs. WORAL enables generating secure and tamper-apparent location provenance products from the given location authority, that have been asserted with a spatio-temporally co-located witness.***

Keywords: Location assertion, location proof, location provenance, location security, witness endorsement, WORAL.

1. INTRODUCTION:

Within this paper, we present WORAL, an entire ready-to-deploy framework for generating and validating witness oriented asserted location provenance records. The WORAL framework is dependent on the asserted location proof protocol and also the OTIT model for generating secure location provenance around the cellular devices. The LA server includes a `Decision Engine', which validates all messages through the protocol. The `Registrar' looks after a tabs on the presently registered witnesses [1]. Ardagna et al. presented obfuscation-based strategies to enable different levels of location privacy according to different the radius of the particular area. Wang et al. suggested STAMP for supplying spatial-temporal probabilistic provenance assurance for mobile users. We make use of the same concept to produce location proofs and also have the proof asserted with a co-located witness. Within this context, a witness is really a spatio-temporally co-located entity using the user and also the location authority. A witness will assert proofs only if willing to do this and may de-register like a witness anytime. The privacy of knowledge inside a proof is uncovered based on the need for the consumer as well as an attacker or auditor should be unable to view any personal data not supposed to have been uncovered through the user. The devices have local storage for storing the provenance products. An area runs a Wireless network, and also the LA is directly attached to the network. Any user interested to get an asserted location provenance record obtains the address from the LA in the site via network broadcasts [2]. The various steps and phases from the protocol happen to be designed, so that, to guarantee the location proof is resistant against collusion attacks and also the provenance from the location proofs is preserved. The consumer then stores the proof info on his device for that specific site S and therefore, completes the secure location provenance protocol. Subsequently, the LA stores the receipts for that location proofs sent in the users. Time for you to complete the entire location proof generation process is an extremely crucial factor when it comes to usability and practicality. The consumer might stay sooner or later for any very short time. The inward and outward arrows show the constituents that are in listening way of accepting messages or have the effect of delivering a note. We used the RSA for generating signatures as well as for all file encryption and understanding from the packets. The settings are instantly synced using the company. The `Service Listener' accepts assertion demands in the LA, and verification demands from another user. The

witness application also utilizes a `Decision Engine', which validates all demands and 'talks' to the `ALP Provider', or even the `VReq Provider' accordingly. However, the witness application doesn't store the data in the messages within the protocol.

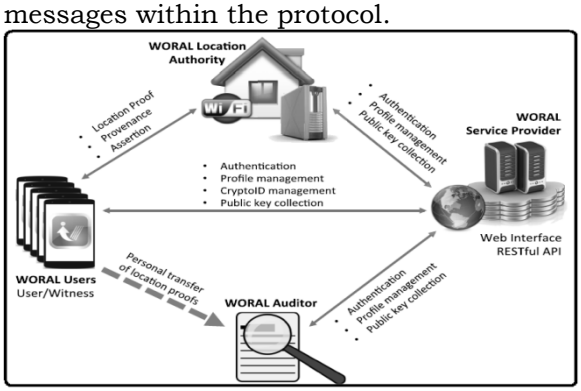


Fig.1.System architecture

2. METHODOLOGY:

A localization authority since the area utilizes some secure distance-bounding mechanism to guarantee the user's presence once the user demands for any location proof. Whenever a user or witness needs the LA's information, it broadcasts a UDP packet to some specific port requesting the data of los angels. The LA always listens for brand new UDP broadcast packets. The implementation from the ready-to-deploy WORAL framework and it is components are described. The operator may use the buttons to stop and start the server, and examine the present listing of location proof receipts. The continuing messages for that protocol is shown on the logging window. An auditor can later verify the claim of presence with regards to the user's identity, the place under consideration, and also the time once the user was present at this location.

The entire mechanism of asserted proofing might be found in a reversed witness oriented application [3]. Rather of the user presenting the proofs as proof of presence, witnesses can instruct notarized records like a evidence of specific users going to a certain location. Models involving more entities normally want more time. Furthermore, additionally, it boosts the dimension of threats. Ananthanarayanan et al. presented StarTrack, a framework in which the sequence of the user's location and time records are kept in tracks [5]. While tracks act like location provenance chains, security issues aren't considered here making tracks susceptible to attacks by malicious users. Inside a commercially deployed scenario, the motivation from the witness could be according to awarded `points' based on valid assertions. The `points' would increase the trust worth of a witness and could be redeemed for membership advantages of the company. The SP may be the only centralized entity within the WORAL architecture that is responsible to handle the accounts from the other three entities, provide authentication, and distribute public keys.

A person can make multiple Crypto-IDs for WORAL and also the user can chose another at different occasions around the mobile phone while requesting the place proof. The LA must maintain a summary of available co-located WORAL mobile users who're interested for everyone as witnesses. While verifying the place proofs supplied by the consumer, the auditor blogs about the plaintext information using the information which is signed through the LA and also the W. The provenance plan PS selected through the user will define the way the information will be employed to produce the new provenance entry [5]. We declare that any distributed security protocol without centralized monitoring requires a minimum of one entity to become valid. The effective completing any security protocol remains safe and secure from the legitimate entity, which plays the function from the situational verifier [6]. We extended our WORAL framework by applying a Google Glass based interface for that WORAL Android user application. The wearable device extension greatly improves the usability from the system by permitting a person to non-intrusively communicate with the WORAL framework with no physical operation around the mobile phone.

3. WORAL FRAMEWORK:

Our solution emphasizes the device's presence, and could be a very relevant technology for equipment handling companies. At the moment, most high finish devices include networking features and built-in memory. The WORAL framework includes a web-based company, desktop-based location authority server, an Android-based user application together with a Google Glass client for that mobile application, as well as an auditor application for location provenance

validation. We've tested our application on LG Nexus 4, Samsung Universe Nexus, Samsung Universe S4, Motorola XT875, HTC 1X, HTC Evo 4G, and Motorola MotoGphones with Android.

4. CONCLUSION:

A safe and secure evidence of presence with provenance upkeep can be used to create ad-hoc social systems and community systems. Therefore, a safe and secure, automated, and non-intrusive location proof generation plan fits perfectly because the underlying mechanism for those such LBS.

Within this paper, we present the Witness Oriented Asserted Location provenance (WORAL) framework. The machine is dependent on the Asserted Location Proof (ALP) protocol and incorporates the OTIT model for secure location provenance. The chronological ordering from the proofs ought to be preserved as well as an attacker should be unable to customize the order of proofs within the provenance records. The protocol design and gratification evaluation was performed and presented in details within the Asserted Location Proof paper.

REFERENCES:

[1] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, ``iPhone and iPod location spoo_ng: Attacks on public WLAN-based positioning systems,'' System Security Group, ETH Zürich Univ., Zürich, Switzerland, Tech. Rep. 599, Apr. 2008.

[2] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, ``Locationbased trust for mobile user-generated content: Applications, challenges and implementations,'' in Proc. HotMobile, Feb. 2008, pp. 60_64.

[3] D. E. Denning and P. F. MacDoran, ``Location-based authentication: Grounding cyberspace for better security,'' Comput. Fraud Secur., vol. 1996, no. 2, pp. 12_16, Feb. 1996.

[4] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer, ``Integrity regions: Authentication through presence in wireless networks,'' IEEE Trans. Mobile Comput., vol. 9, no. 11, pp. 1608_1621, Nov. 2010.

[5] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, ``Location privacy protection through obfuscationbased techniques,'' in Data and Applications Security. Berlin, Germany: Springer-Verlag, 2007, pp. 47_60.

[6] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer, ``Integrity regions: Authentication through presence in wireless networks,'' IEEE Trans. Mobile Comput., vol. 9, no. 11, pp. 1608_1621, Nov. 201

A WIDE RANGE ROAD NETWORK NAVIGATOR FOR LOCATION SEARCH

Mr.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 III Year CSE, (16RG1A0537, 16RG1A0530, 16RG1A0536, 16RG1A0548), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT: ***To facilitate quick recognition of PPatterns, rather of exhaustively checking all of the queried pathways in cache, we design a grid-based index for that PPattern Recognition module. According to these detected PPatterns, the Shortest Path Estimation module constructs candidate pathways for that new query and chooses the right one. Path planning, a simple purpose of road network navigation services, finds a route between your specified start location and destination. The efficiency of the path planning function is crucial for mobile users on roads because of various dynamic scenarios, like a sudden alternation in driving direction, unpredicted traffic conditions, lost or unstable Gps navigation signals, and so forth. During these scenarios, the road planning service must be delivered in due time. Within this paper, we advise a method, namely, Path Planning by Caching (PPC), to reply to a brand new path planning query instantly by efficiently caching and reusing historic queried-pathways. Unlike the traditional cache-based path planning systems, in which a queried-path in cache can be used only if it matches perfectly using the new query, PPC leverages the partly matched queries to reply to part(s) from the new query. Consequently, the server only must compute the unmatched path segments, thus considerably lowering the overall system workload. Since the unmatched segments are often merely a smaller sized area of the original query, the server only processes a "smaller sub query", having a reduced workload. After we return the believed road to the consumer, the Cache Management module is triggered to find out which queried-pathways in cache ought to be evicted when the cache is full..***

Keywords: Pattern Detection Module, Spatial database, path planning, cache management, GPS..

1. INTRODUCTION:

In mobile navigation services, on-road path planning is really a fundamental function that finds a route from a queried start location along with a destination. During roads, a way planning query might be issued because of dynamic factors in a variety of scenarios. we advise a method, namely, Path Planning by Caching (PPC) that aims to reply to a brand new path planning query efficiently by caching and reusing in the past queried pathways [1]. The thought of PPatterns is dependent on an observation that similar beginning and destination nodes of two queries may lead to similar shortest pathways. With an empirical study, we discover that common road segments in a variety of queried-pathways will often have road kinds of greater importance and capacity. We've created a new cache substitute mechanism by thinking about the consumer preference among roads of numerous types. We advise a cutting-edge system, namely, path planning by caching. Because of the wide accessibility to the gps (Gps navigation) and digital mapping of roads, road network navigation services have grown to be a fundamental application on the majority of cellular devices.

Literature Overview: Jung and Pramanik propose the HiTi graph model to structure a sizable road network model. HiTi aims to lessen looking space for that shortest path computation. The formula of the benefit value views two features: the recognition of the path and it is expense. The recognition of the path p is evaluated in line with the quantity of occurrences from the historic sub pathways which overlap p. Gutman propose a achieve-based method for computing the shortest pathways. A better version adds shortcut arcs to lessen vertices from being visited and uses partial trees to lessen the preprocessing time [2]. To be able to enhance the retrieval efficiency from the path planning system, Thomsen et al. propose a brand new cache management policy. Mahmud et al. propose a group based method of accelerate the processing by calculating the similarity among several queries and send the most popular part like a query towards the server.

2. TRADITIONAL APPROACH:

Path planning must be delivered in due time. The advantages of timeliness is much more challenging when a massive quantity of path planning queries is posted towards the server, e.g., during peak hrs. Because the response

time is crucial to user satisfaction with personal navigation services, it's a mandate for that server to efficiently handle the heavy workload of path planning demands. Jung and Pramanik propose the HiTi graph model to structure a sizable road network model. HiTi aims to lessen looking space for that shortest path computation. While HiTi achieves high end on road weight updates and reduces storage overheads, it incurs greater computation costs when computing the shortest pathways compared to HEPV and also the Hub Indexing methods [3]. To compute time-dependent fast pathways, Demiryurek et al. propose the B-TDFP formula by leveraging backward searches to lessen looking space. It adopts a place-level partition plan which relies on a road hierarchy to balance each area. Disadvantages of existing system: A cached totally came back only if it matches completely with a brand new query. Time complexity is high. The cache content might not be current to reply to recent trends in issued queries. The price of setting up a cache is high, because the system must calculate the advantage values for those sub-pathways inside a full-road to query results.

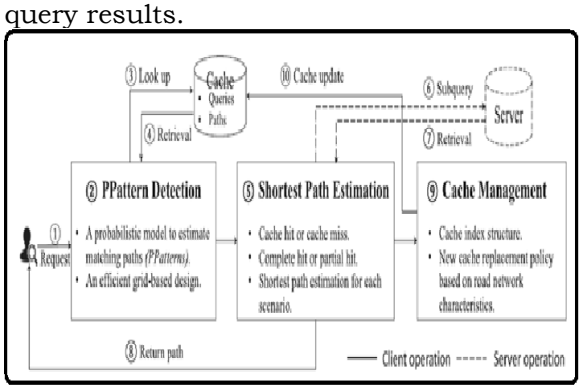


Fig.1.Framework of proposed system.

3. ENHANCED METHOD:

To satisfy existing need, we advise a method, namely, Path Planning by Caching (PPC) that aims to reply to a brand new path planning query efficiently by caching and reusing in the past queried pathways. The suggested system includes three primary components: (i) PPattern Recognition,(ii) Shortest Path Estimation, and (iii) Cache Management. Given a way planning query, containing a resource location along with a destination location, PPC first of all determines and retrieves numerous historic pathways in cache, known as PPatterns that could match this latest query rich in probability. The thought of PPatterns is dependent on an observation that similar beginning and destination nodes of two queries may lead to similar shortest pathways. Comprehensive experimentation on the real road network database implies that our bodies outperform the condition-of-the-art path planning techniques by reduction of 32 percent from the computation latency typically. Within the component PPatern Recognition, we advise a singular probabilistic model to estimate the chance for any cached queried-road to be helpful for answering the brand new query by exploring their geospatial characteristics [4]. Within this component, if your PPattern perfectly matches the query, we immediately give it back towards the user otherwise, the server is requested to compute the unmatched path segments between your PPattern and also the query. A fundamental part of this module is really a new cache substitute policy which considers the initial characteristics of road systems. Benefits of suggested system: PPC leverages partly matched queried-pathways in cache to reply to part(s) from the new query. Consequently, the server only must compute the unmatched path segments, thus considerably lowering the overall system workload. We advise a cutting-edge system, namely, path planning by caching, to efficiently answer a brand new path planning query by utilizing cached pathways to prevent having a time-consuming shortest path computation. Typically, we conserve to 32 percent of your time in comparison to a standard path planning system. We introduce the idea of PPattern, i.e., a cached path which shares segments along with other pathways. PPC supports partial hits between PPatterns along with a new query. Our experiments indicate that partial hits constitute as much as 92.14 % of cache hits typically. A singular probabilistic model is suggested to identify the cached pathways which are of high probability to become a PPattern for that new query in line with the coherency property from the road systems. Our experiments indicate these PPatterns save retrieval of path nodes by 31.69 percent typically, representing a10-fold improvement within the 3.04 percent saving achieved with a complete hit. We've created a new cache substitute mechanism by thinking about the consumer preference among roads of numerous types [5]. A usability measure is assigned for every query by addressing both road type and query recognition.

Fundamental Statements: However, because of the dependence on timeliness, the performance of the path planning services is evaluated when it comes to both distance and response time. Unlike the traditional cache-based path planning systems, in which a queried-path in cache can be used only if it matches perfectly using the new query, PPC leverages the partly matched cached queries to reply to part(s) of the new query. The cache substitute policy aims to enhance the hit ratio and lower access latency. An intuitive option would be to check on whether there's a cached queried-path perfectly matching the brand new query. Because the unshared segment is shorter compared to original path, the computational overhead might be considerably reduced. Consequently, the server workload is considerably reduced.

Recognition Framework: To identify the very best PPatterns, a concept would be to calculate the estimation distance according to each cached path. Several existing research has suggested algorithms to group pathways concentrating on the same trajectories together. Differing in the existing studies, we advise a means to identify the possibility PPatterns to have an input query only using existing pathways in cache. The coherency property of road systems signifies that two pathways are certainly going to share segments while source nodes are near to one another. the ultimate probability could be computed because the product of those three terms [6]. Within the first scenario, there is a minimum of one common segment between your pathways of these two queries. Within the other two scenarios, there are no common segments. The primary idea would be to divide the entire space into equally sized grid cells. Only then do we locate the grid cells, we'll discuss the cache index.

Shortest Path Estimation: The cached pathways whose source and destination nodes come in the origin grid cell and destination grid cell, where versus and vt from the new query can be found, could be immediately acquired without contacting the server. To enhance the performance, we adopt an approximation distance by calculating the Euclidean distance between your source-source and destination-destination nodes. The cache maintains two tables to have an efficient cache lookup. The very first table records each grid-cell by which pathways have passed. This table enables quick identification of potential PPatterns for that new query. The 2nd table records all nodes of every path within their traveling order. In road systems, observe that certain routes are often liked by users. Within this paper, we advise a method, namely, Path Planning by Caching, to reply to a brand new path planning query with rapid response by efficiently caching and reusing the historic queried-pathways [7]. Generally, having a greater hit ratio, the machine performance improves too. The inconsistency above is especially apparent in PPC, most likely because PPC leverages partial hits to reply to a brand new query. PPC adopts a grid-based means to fix identify the possibility PPatterns for any new query, so how big the grid-cell directly impacts the hit ratio and also the system performance. We realize that as cache size increases, the machine saves more visited nodes and query time, however with a bigger deviation percentage.

4. CONCLUSION:

We conduct an extensive performance look at the suggested PPC system while using road network dataset. Comprehensive experimentation on the real road network database implies that our bodies outperform the condition-of-the-art path planning techniques by reduction of 32 percent from the computational latency typically. Within this paper, we offer a brand new framework for reusing the formerly cached query results plus an effective formula for increasing the query evaluation around the server. We first of all at random produce a query are the initial navigational route. Next, we at random draw a probability to look for the opportunity for a person to alter direction. Consequently, the server only must compute the unmatched segments, thus considerably lowering the overall system workload. The cache substitute policy aims to enhance the hit ratio and lower access latency. An intuitive option would be to check on whether there's a cached queried-path perfectly matching the brand new query. The experimental results reveal that our new cache substitute policy boosts the overall cache hit ratio by 25.02 percent within the condition-of-the-art cache substitute policies.

REFERENCES:

[1] Ying Zhang, Member, IEEE, Yu-Ling Hsueh, Member, IEEE,Wang-Chien Lee, Member, IEEE, and Yi-HaoJhang, “Efficient Cache-Supported PathPlanning on Roads”, ieee transactions on knowledge and data engineering, vol. 28, no. 4, april 2016.

[2] X. Xiong, M. F. Mokbel, and W. G. Aref, "SEA-CNN: Scalable processing of continuous k-nearest neighbor queries in spatiotemporal databases," in Proc. IEEE 21st Int. Conf. Data Eng., 2005, pp. 643–654.

[3] A. V. Goldberg and C. Silverstein, "Implementations of Dijkstra's algorithm based on multi-level buckets," Network Optimization, vol. 450, pp. 292–327, 1997.

[4] S. Jung and S. Pramanik, "An efficient path computation model for hierarchically structured topographical road maps," IEEE Trans. Knowl. Data Eng., vol. 14, no. 5, pp. 1029–1046, Sep. 2002.

[5] H. Gonzalez, J. Han, X. Li, M. Myslinska, and J. P. Sondag, "Adaptive fastest path computation on a road network: A traffic mining approach," in Proc. 33rd Int. Conf. Very Large Data Bases, 2007, pp. 794–805.

[6] R. Ozcan, I. S. Altingovde, B. B. Cambazoglu, F. P. Junqueira, and zgr Ulusoy, "A five-level static cache architecture for web search engines," Inf. Process. Manage., vol. 48, no. 5, pp. 828–840, 2012.

[7] R. Ozcan, I. S. Altingovde, and O. Ulusoy, "A cost-aware strategy for query result caching in web search engines," in Proc. Adv. Inf. Retrieval, 2009, vol. 5478, pp. 628–636.

1.

AN AUTO-PROTECTIVE DIGGING TECHNIQUE FOR FLAWS

Mr.CH.V.Krishna Mohan[1]., K Spandhana[2]., B 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 III Year CSE, (16RG1A0543, 16RG1A0508, 16RG1A0510, 16RG1A0528),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT: ***Perhaps, grounds for that insecurity of web applications is the fact that many programmers lack appropriate understanding about secure coding, so that they leave applications with flaws. This paper explores a strategy for instantly protecting web applications and keep the programmer informed. The approach consists in analyzing the net application source code trying to find input validation vulnerabilities, and inserting fixes within the same code to fix these flaws. research from the configuration from the data mining component, as well as an experimental look at the tool with a number of free PHP applications. The tool may be extended with increased flaws and databases, however this set is sufficient to demonstrate the idea. Designing and applying WAP would be a challenging task. Unlike our work, other works didn't try to identify bugs and identify their whereabouts, but to evaluate the caliber of the program with regards to the prevalence of defects and vulnerabilities. The tool does taint analysis of PHP programs, a kind of data flow analysis. Within the first four posts on the table would be the decision tree models. These models select for that tree nodes the attributes which have greater information gain. The C4.5/J48 model prunes the tree to attain better results. The K-NN model has far better performance since the courses are now balanced. However, the kappa, precision, and precision metrics reveal that the Bayes models continue being the worst.***

Keywords: Data mining, web protection, input validation vulnerabilities, software security, source code static analysis, web applications, PHP.

. 1. INTRODUCTION:

A fundamental part of this problem stems from vulnerable source code, frequently designed in unsafe languages like PHP. The approach suggested is, therefore, about information-flow security poor web applications. We're mostly worried about the server-side of those applications that is normally designed in a language for example PHP, Java, or Perl. They classify an incident within the class which has the greatest probability. NB is a straightforward probabilistic classifier according to Bayes' theorem, in line with the assumption of conditional independence from the probability distributions from the attributes [1]Kay-NN classifies an incident within the type of its neighbors. LR uses regression analysis to classify an incident. For stored XSS, the sanitization function add slashes can be used, and also the validation process verifies in runtime if the attempt of exploitation occurs, raising a security if that's the situation. Of these two classes of vulnerabilities, a fix is placed for every malicious input that will reach a sensitive sink. Therefore, the issue is a situation of language-based information-flow. Source code static analysis tools are a strategy to find vulnerabilities, however they have a tendency to generate false positives, and wish considerable effort for programmers to by hand fix the code. Validation involves examining the data, and executing the sensitive sink or otherwise based on this verification. Most fixes are placed within the type of the sensitive sink rather of, for instance, the road from the access point, to prevent interference along with other code that sanitizes the variable. Sanitization depends upon the sensitive sink, i.e., around the means by that the input can be used. For SQL, and also the MySQL database, PHP offers the mysql_real_escape_string function [2]. To summarize study regarding the very best classifier, we have to understand which attributes lead most to some candidate vulnerability as being a false positive. For your purpose, we obtained from our data set 32 false positive instances, and classified them in three sub-classes, one for each one of the teams of attributes.

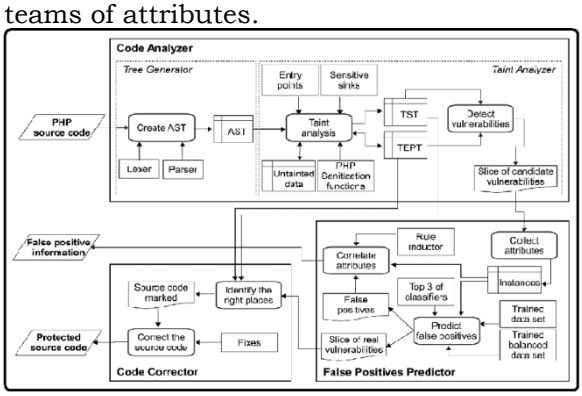


Fig.1.Proposed system framework

2. METHODOLOGY:

The code analyzer first parses the PHP source code, and generates an AST. Then, it uses tree walkers to complete taint analysis, i.e., to trace if data provided by users with the entry ways reaches sensitive sinks without sanitization. Throughout the analysis, each time a variable that's passed to some sensitive sink becomes tainted, the false positives predictor is activated to gather the vector of attributes, creating thus an incident, and classify the instance like a false positive or perhaps a real vulnerability [3]. The static analysis issue is undividable, and relying on data mining cannot circumvent this undesirability, only provide probabilistic results. The tool corrects the code by inserting fixes, i.e., sanitization and validation functions. Tests are accustomed to verify when the fixes really take away the vulnerabilities and don't compromise the (correct) behavior from the applications. While carrying this out analysis, the code analyzer generates tainted symbol tables and tainted execution path trees for individual's pathways that link entry ways to sensitive sinks without correct sanitization. The code corrector picks the pathways considered true positives to signal the tainted inputs to become sanitized while using tables and trees pointed out above [4]. Case study may be further refined by thinking about, for instance, the semantics of string manipulation functions. However, coding clearly more understanding inside a static analysis tool is difficult, and frequently needs to be accomplished for each type of vulnerabilities. We combine taint analysis, which finds candidate vulnerabilities, with data mining, to calculate the presence of false positives. To calculate the presence of false positives, we introduce the novel concept of assessing when the vulnerabilities detected are false positives using data mining. To get this done assessment, we measure features of the code that people observed to become connected with the existence of false positives, and employ a mix of the 3 top-ranking classifiers to flag every vulnerability as false positive or otherwise. acquiring attributes in the candidate vulnerable control-flow pathways, and taking advantage of the very best 3 classifiers to calculate if each candidate vulnerability is really a false positive or otherwise. The taint analyzer is really a static analysis tool that operates over an AST produced with a laxer along with a parser, for PHP 5 within our situation. In the existence of an incorrect positive, use induction rules to provide the relation between your attributes that classified it. The taint analyzer flags a vulnerability when the data flow isn't untainted with a sanitization function before reaching the sensitive sink. These string manipulation functions may lead to the sanitization of the data flow, however the taint analyzer doesn't have enough understanding to alter the status from tainted to untainted, therefore if a vulnerability is flagged it might be an incorrect positive. The attack involves convincing the consumer to click a hyperlink that accesses the net application, delivering it a script that's reflected through the echo instruction and performed within the browser [5]. This sort of attack could be avoided by sanitizing the input, or by encoding the output, or both. Our results claim that the tool is capable of doing finding and correcting the vulnerabilities in the classes it had been developed to handle. This method includes two approaches which are apparently orthogonal: humans coding the understanding about vulnerabilities, became a member of using the apparently orthogonal approach of instantly acquiring that understanding. greater assurance could be acquired with two types of testing, particularly program mutation to ensure when the fixes do their function, and regression testing to ensure when the behavior from the application continues to be the same goes with benign inputs. Our approach involves doing code correction instantly following the recognition from the vulnerabilities is conducted through the taint analyzer and also the data mining component [6]. The taint analyzer returns data concerning the vulnerability, including its class, and also the vulnerable slice of code. Each branch from the TEPT matches a tainted variable, and possesses a sub-branch for every type of code in which the variable becomes tainted. We identified the attributes by analyzing by hand some vulnerabilities discovered by WAP's taint analyzer. We studied these vulnerabilities to know when they were false positives. This research involved both studying the origin code, and executing attacks against each vulnerability found to know whether it was attackable or otherwise. Data mining is usually about correlation, however the classifiers presented to date don't show this correlation. For your purpose, our machine learning approach enables us to recognize mixtures of attributes which are correlated with the existence of false positives, i.e., what attributes justify the classification of false positives. The records within the sub branches

would be the variables the tainted variable propagated its condition into. Taint analysis involves updating the TEPT using the variables that become tainted. WEKA enables us to get this done using meta-models. Within the evaluation made in the last section, the Random Tree (RT) and LR were two best classifiers. We used the Bagging, Stacking, and Boosting algorithms with RT and Boosting with LR. The approach and also the tool look for vulnerabilities using a mix of two techniques: static source code analysis, and knowledge mining [7]. Data mining can be used to recognize false positives while using best three machine learning classifiers, and also to justify their presence utilizing an induction rule classifier.

3. PHP APPLICATIONS:

Our approach was implemented within the WAP tool, as well as an experimental evaluation was performed having a large group of PHP applications. This method contributes straight to the safety of web applications by removing vulnerabilities, and not directly allowing the programmers study from their mistakes. choose a representative group of vulnerabilities recognized by the taint analyzer, verify if they're false positives or otherwise, extract some attributes, evaluate their record correlation with the existence of an incorrect positive, evaluate candidate classifiers to pick the right for that situation in point, and define the parameters from the classifier.

4. CONCLUSION:

This last aspect is enabled by inserting fixes such as the following common security coding practices, so programmers can learn these practices by seeing the vulnerabilities, and just how these were removed. WAP also does taint analysis and alias analysis for discovering vulnerabilities, even though it goes further by also correcting the code. In addition, Pixy does only module-level analysis, whereas WAP does global analysis.

REFERENCES:

[1] G. T. Buehrer, B. W. Weide, and P. Sivilotti, “Using parse tree validation to prevent SQL injection attacks,” in Proc. 5th Int. Workshop Software Engineering and Middleware, Sep. 2005, pp. 106–113.

[2] N. Jovanovic, C. Kruegel, and E. Kirda, “Precise alias analysis for static detection of web application vulnerabilities,” inProc. 2006Workshop Programming Languages and Analysis for Security, Jun. 2006, pp. 27–36.

[3] G. Wassermann and Z. Su, “Sound and precise analysis of web applications for injection vulnerabilities,” in Proc. 28th ACM SIGPLAN Conf. Programming Language Design and Implementation, 2007, pp. 32–41.

[4] E. Arisholm, L. C. Briand, and E. B. Johannessen, “A systematic and comprehensive investigation of methods to build and evaluate fault prediction models,” J. Syst. Softw., vol. 83, no. 1, pp. 2–17, 2010.

[5] L. K. Shar and H. B. K. Tan, “Mining input sanitization patterns for predicting SQL injection and cross site scripting vulnerabilities,” in Proc. 34th Int. Conf. Software Engineering, 2012, pp. 1293–1296.

[6] T. Pietraszek and C. V. Berghe, “Defending against injection attacks through context-sensitive string evaluation,” in Proc. 8th Int. Conf. Recent Advances in Intrusion Detection, 2005, pp. 124–145.

[7] S. Lessmann, B. Baesens, C. Mues, and S. Pietsch, “Benchmarking classification models for software defect prediction: A proposed framework and novel findings,” IEEE Trans. Softw. Eng., vol. 34, no. 4, pp. 485–496, 2008.

AN INFERENCE PREVENTIVE TECHNIQUE FOR GENERAL TRAFFIC ANALYSIS

Mrs.G.Sujatha[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 III Year CSE, (16RG1A0507, 16RG1A0503, 16RG1A0524, 16RG1A0526),
Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

ABSTRACT: ***Contextual information could be uncovered by eavesdropping on over-the-air transmissions and acquiring transmission attributes, for example inter-packet occasions, packet source and destination IDs, and number and sizes of transmitted packets. Leakage of contextual information poses a significant threat towards the WSN mission and operation. We developed two algorithms for partitioning the WSN to MCDSs and SS-MCDSs and evaluated their performance via simulations. When compared with prior methods able to avoiding a worldwide eavesdropper, we demonstrated that restricting the dummy traffic transmissions to MCDS nodes, cuts down on the communication overhead because of traffic normalization. Within the military surveillance scenario, the foe can link the occasions detected through the WSN to compromised assets. We highlight our goal isn't to produce probably the most sophisticated attack. This kind of attack is extremely-determined by the security mechanism and could require additional a priori understanding. First, eavesdroppers are passive devices which are difficult to identify. Second, the supply of low-cost commodity radio hardware causes it to be affordable to deploy a lot of eavesdroppers. Third, even when file encryption is used to hide the packet payload, some fields within the packet headers still need be transmitted within the obvious for proper protocol operation. We advise a heuristic formula that computes an approximation of V's partition by balancing between your appearance frequency, the amount of MCDSs that span V, and also the MCDS size.***

Keywords: Eavesdropping, contextual information, privacy, anonymity, graph theory, heuristic algorithm.

1. INTRODUCTION:

The origin forwards a packet to some at random selected neighbor one way. This neighbor is constantly on the forward the packet very much the same, however in the alternative direction. The operation is repeated until h hops are traversed. Within the second stage, the packet is given to the sink using probabilistic flooding [1]. Each tag set is connected having a sensor label that is representative of the transmissions inside the particular area. Our method depends on minimal information, namely packet transmission some time and eavesdropping location. To lessen the forwarding delay we schedule sensors to deliver in accordance with their depth within the CDS tree, once the tree is assumed to become rooted in the sink. To have an interval T, if downstream nodes are scheduled to deliver after upstream ones, a genuine transmission is certain to achieve the sink within T: We highlight the coordination enforced by DFAS conceals the traffic direction. A nearby foe can intercept a restricted quantity of transmissions inside the WSN. The confidentiality from the report remains safe and secure using standard cryptographic methods. Packet transmissions are re-encrypted on the per-hop basis to avoid tracing of relayed packets. Sensors know about their one- and 2-hop neighbors using a neighbor discovery service [2]. Even without the eavesdropper location information, one must take into account all possible eavesdropping locations to supply privacy guarantees, which is the same as a worldwide adversarial model. We address the issue of stopping the inference of contextual information in the event-driven wireless sensor systems (WSNs). The issue is considered within global eavesdropper who analyzes low-level RF transmission attributes, like the quantity of transmitted packets, inter-packet occasions, and traffic directionality, to infer event location, its occurrence time, and also the sink location. We devise an over-all traffic analysis way of inferring contextual information by correlating transmission occasions with eavesdropping locations. Our analysis implies that most existing countermeasures either neglect to provide sufficient protection, or incur high communication and delay overheads.

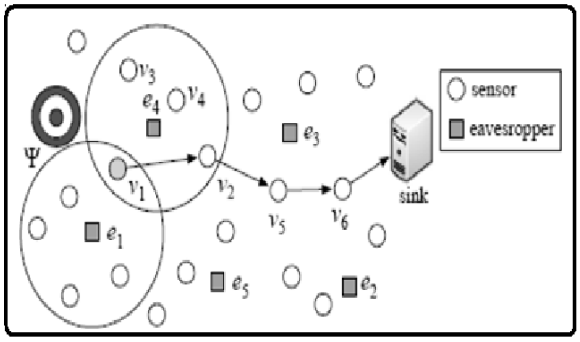


Fig.1.System architecture

2. PROPOSED MODEL:

We advise resource-efficient traffic normalization schemes. As compared to the condition-of-the-art, our methods lessen the communication overhead by greater than 50% and also the finish-to finish delay by greater than 30%. To do this, we partition the WSN to minimum connected dominating sets that be employed in a round-robin fashion [3]. This enables us to lessen the amount of traffic sources active in a with time, while supplying routing pathways to the node within the WSN. We further reduce packet delay by loosely coordinating packet relaying, without revealing the traffic directionality. The issue is considered within global eavesdropper who analyzes low-level RF transmission attributes, like the quantity of transmitted packets, inter-packet occasions, and traffic directionality, to infer event location, its occurrence time, and also the sink location. We advise traffic normalization techniques that hide the big event location, its occurrence time, and also the sink location from global eavesdroppers. When compared with existing approaches, our methods lessen the communication and delay overheads by restricting the injected bogus traffic [4]. The technique is agnostic towards the protection mechanism and can be used set up a baseline for evaluating different schemes. To mitigate global eavesdropping, we suggested traffic normalization techniques that regulate the sensor traffic patterns of the subset of sensors that form MCDSs. We evaluate this privacy because the distance between your deduced location according to O(W) and the position of the source. Just one subset is active in a given epoch, and subsets are periodically rotated inside a round-robin fashion. A sensor is permitted to transmit traffic (bogus or real) only when a subset it is associated with is active. Our technique is meant like a baseline for evaluating the performance of protection mechanisms with different underlying assumptions. The division depends upon the temporal and spatial tag correlation. For example, consider packets p1 and p2 from v and u in V: Top of the bound associate's transmissions that occur near the coast some time and wide with similar event. We observe that the foe could apply other record analysis methods, for example individuals reported [5]. These techniques neglect to identify, because the transmission patterns of sensors in Di don't change when real visitors are introduced. We think that synchronization is maintained for purposes that stretch past the privacy of contextual information such as the implementation of well-known time-slotted protocols in the MAC layer and temporal analysis of sensor data in the sink. Both thresholds were selected presuming dense deployments by which pathways could be approximated by straight lines. Since the operation is initiated within the leader's neighborhood, using the change of the grey node into black, each dominated black node is attached to the leader. To help lessen the forwarding delay, we loosely coordinate sensor transmissions according to tree structures. Our traffic normalization plan contain a network partition along with a transmission coordination phase. The CDS property guarantees that a minimum of one node in Dj would overhear the final relay of m with a node in Di [6]. We create a simple routing plan to forward packets over multiple CDSs.

3. TRAFFIC NORMALIZATION SCHEMES:

Our analysis implies that most existing countermeasures either neglect to provide sufficient protection, or incur high communication and delay overheads. To mitigate the outcome of eavesdropping, we advise resource-efficient traffic normalization schemes. As compared to the condition-of-the-art, our methods lessen the communication overhead by greater than 50% and also the finish-to finish delay by greater than 30%.Our technique is agnostic towards the network topology (although it is deduced) and also to the particular mechanism accustomed to counter traffic analysis, in order that it could be broadly applied.

4. CONCLUSION:

To lessen the forwarding delay, we design an interest rate control plan that loosely coordinates sensor transmissions over multi-hop pathways without revealing real traffic patterns or even the traffic directionality. The WSN needs to transmit V bogus messages

periodically to normalize the traffic patterns each and every sensor, whereas the WSN partition to sub graphs needs to be applied just once. The MCFS operation impacts the finish-to-finish delay for delivering a study towards the sink in 2 ways.

REFERENCES:

[1] M. Mahmoud and X. Shen. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 23(10):1805–1818, 2012.

[2] M. Fruth. Probabilistic model checking of contention resolution in the IEEE 802.15.4 low-rate wireless personal area network protocol. In Proc. of the Symp. on Leveraging Applications of Formal Methods, Verification and Validation, pages 290–297, 2006.

[3] Y. Xi, L. Schwiebert, and W. Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In Proc. Of the Parallel and Distributed Processing Symposium, pages 1–8, 2006.

[4] G. Chinnu and N. Dhinakaran. Protecting location privacy in wireless sensor networks against a local eavesdropper–a survey. International Journal of Computer Applications, 56(5):25–47, 2012.

[5] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proc. of the ACM Conference on Mobile Systems, Spplications, and Services, pages 40–53, 2008.

[6] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran. Toward a statistical framework for source anonymity in sensor networks. IEEE Transactions on Mobile Computing, 12(2):248–260, 2013.

AN OUTSOURCED APPRAISAL POLICY FOR IN-DEPTH IMITATION DEFENCE SCHEME

K Sheetal[1] .,K Pallavi[2]., K Supraja[3]., G Niharika[4] ., D Anusha[5]

1 Assistant 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 III Year CSE, (16RG1A0542, 16RG1A0550, 16RG1A0532, 16RG1A0515),

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

ABSTRACT: ***Within this paradigm, key updates could be securely outsourced with an approved party, and therefore the important thing-update burden around the client is going to be stored minimal. Within this paper, we focus regarding how to result in the key updates as transparent as you possibly can for that client and propose a brand new paradigm known as cloud storage auditing with verifiable outsourcing of key updates. Besides, our design also equips the customer with capacity to help verify the validity from the encrypted secret keys supplied by the OA. Particularly, we leverage the outsourced auditor in lots of existing public auditing designs; allow it to act as approved party within our situation, making it responsible for both storage auditing and also the secure key updates for key-exposure resistance. We formalize the meaning and also the security type of this paradigm. The approved party holds an encrypted secret key from the client for cloud storage auditing and updates it underneath the encrypted condition in every period of time. The customer downloads the encrypted secret key in the approved party and decrypts it just as he wants to upload new files to cloud. Within our design, OA only must hold an encrypted form of the client's secret key while doing each one of these troublesome tasks with respect to the customer. The customer only must download the encrypted secret key in the OA when uploading new files to cloud. Within our design, OA only must hold an encrypted form of the client's secret key while doing each one of these troublesome tasks with respect to the customer.***

Keywords: Outsourced Auditor (OA), outsourcing computing, cloud storage auditing.

1. INTRODUCTION:

We advise a brand new paradigm known as cloud storage auditing with verifiable outsourcing of key updates. We design the very first cloud storage auditing protocol with verifiable outsourcing of key updates. These protocols concentrate on different factors of cloud storage auditing like the high quality, the privacy protection of information, the privacy protection of identities, dynamic data operations, the information discussing, etc. Yu et al. built a cloud storage auditing protocol with key-exposure resilience by updating the user's secret keys periodically. Recently, outsourcing computation has attracted much attention and been researched broadly. An important security problem is how you can efficiently look into the integrity from the data kept in cloud. Recently, many auditing protocols for cloud storage happen to be suggested to cope with this issue [1]. Cloud storage is globally viewed among the most significant services of cloud-computing. Although cloud storage provides significant advantage to users, it brings new security challenging problems. It earns new local burdens for that client since the client needs to execute the important thing update formula in every period of time to create his secret key move ahead. However, it must satisfy several new needs to do this goal. First of all, the actual client's secret keys for cloud storage auditing shouldn't be known through the approved party who performs outsourcing computation for key updates. Lately, how to approach the important thing exposure issue in the settings of cloud storage auditing continues to be suggested and studied. To deal with the task, existing solutions all require client to update his secret keys in each and every period of time, which might inevitably generate new local burdens towards the client, especially individuals with limited computation sources, for example cell phones. Key-exposure resistance happens to be an essential problem for in-depth cyber defense in lots of security applications. Otherwise, it'll bring the brand new security threat. Therefore the approved party must only hold an encrypted form of the user's secret key for cloud storage auditing. Next, since the approved party performing outsourcing computation only knows the encrypted secret keys, key updates ought to be completed underneath the encrypted condition. Thirdly, it ought to be extremely powerful for that client to recuperate the actual secret key in the encrypted version that's retrieved in the approved party. Lastly, the customer will be able to verify the validity from the encrypted secret key following the client retrieves it in the approved party. The aim of this paper would be to design a cloud storage auditing protocol that may satisfy above needs to offer the outsourcing of key updates. We formalize the meaning and also

the security type of the cloud storage auditing protocol with verifiable outsourcing of key updates. We prove the safety in our protocol within the formalized security model and justify its performance by concrete implementation [2].

2. TRADITIONAL SCHEME:

Yu et al. built a cloud storage auditing protocol with key-exposure resilience by updating the user's secret keys periodically. In this manner, the harm of key exposure in cloud storage auditing could be reduced. It earns new local burdens for that client since the client needs to execute the important thing update formula in every period of time to create his secret key move ahead. For many clients with limited computation sources, they may not look forward to such extra computations on their own in every period of time. It might be clearly more appealing to create key updates as transparent as you possibly can for that client, particularly in frequent key update scenarios [2]. Wang et al. suggested an open privacy-preserving auditing protocol. They used the random masking technique to help make the protocol achieve privacy preserving property. Disadvantages of existing system: No verification system readily available for client's for to check on validity from the encrypted secret keys when installing them in the TPA. All existing auditing protocols are built around the assumption the secret key from the client is completely secure and wouldn't be uncovered.

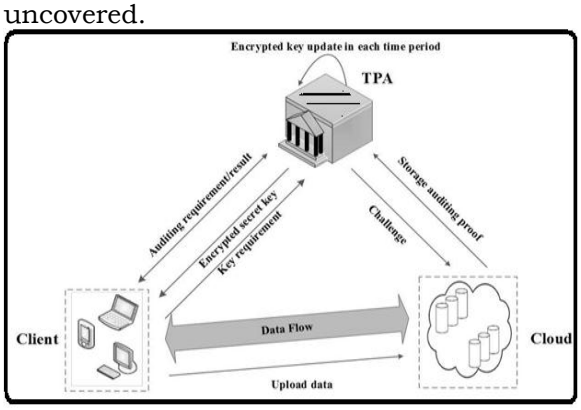


Fig.1.Proposed structure.

3. ENHANCED APPROACH:

We advise a brand new paradigm known as cloud storage auditing with verifiable outsourcing of key updates. Within this new paradigm, key-update operations aren't done by the customer, but by an approved party. Additionally, the customer can verify the validity from the encrypted secret key. We design the very first cloud storage auditing protocol with verifiable outsourcing of key updates. Within our design, the 3rd party auditor (TPA) plays the function from the approved party who manages key updates. We prove the safety in our protocol within the formalized security model and justify its performance by concrete implementation. Benefits of suggested system: The TPA doesn't be aware of real secret key from the client for cloud storage auditing, only holds an encrypted version. Within the detailed protocol, we make use of the blinding technique with homomorphic property to create the file encryption formula to secure the key keys held through the TPA. We formalize the meaning and also the security type of the cloud storage auditing protocol with verifiable outsourcing of key updates. The safety proof and also the performance simulation reveal that our detailed design instantiations are safe and effective. Each one of these salient features is carefully designed to help make the whole auditing procedure with key exposure resistance as transparent as you possibly can for that client [3]. It can make our protocol secure and also the understanding operation efficient. Meanwhile, the TPA can complete key updates underneath the encrypted condition. T in the approved party and decrypts it just as he want to upload new files to cloud. Additionally, the customer can verify the validity from the encrypted secret key. Cloud storage auditing protocol with verifiable outsourcing of key updates. The customer can verify the validity from the encrypted secret key as he retrieves it in the TPA. The safety type of the cloud storage auditing protocol with verifiable outsourcing of key updates.

Preliminaries: We use three games to explain the adversaries with various compromising abilities who're from the security from the suggested protocol. Game 1 describes a foe, which fully compromises the OA to obtain all encrypted secret keys. Game 2 describes a foe, which compromises the customer to obtain DK, attempts to forge a legitimate authenticator in almost any period of time. Game 3 offers the foe more abilities, which describes a foe, which compromises the customer and also the OA to obtain both Ask and DK previously period j, attempts to forge a legitimate authenticator before period of time j. The OA plays two important roles: the very first is to audit the information files kept in cloud for that client the second reason is to update the encrypted secret keys from the client in every period of time. The OA can be viewed as like a party with effective computational capacity or perhaps a service in

another independent cloud. You will find three parties within the model: the customer, the cloud and also the third-party auditor (OA). The customer has the files which are submitted to cloud. The entire size these files isn't fixed, that's, the customer can upload the growing files to cloud in various time points. The cloud stores the client's files and offers download service for that client [4]. Within the finish of every period of time, the OA updates the encrypted client's secret key for cloud storage auditing based on the next time period. The safety model formalizes the adversaries with various reasonable abilities who attempt to cheat the challenger he owns one file he actually doesn't entirely know.

Technical Enhancements: Traditional file encryption strategy is not appropriate since it helps make the key update hard to be completed underneath the encrypted condition. Besides, it will likely be even more complicated to allow the customer using the verification capacity to guarantee the validity from the encrypted secret keys. To deal with these challenges, we advise look around the blinding technique with homomorphic property to efficiently "encrypt" the key keys. We make use of the same binary tree structure to evolve keys that has been accustomed to design several cryptographic schemes [5]. This tree structure could make the protocol achieve fast key updates and short key size. One problem we have to resolve would be that the OA should carry out the outsourcing computations for key updates underneath the condition the OA doesn't be aware of real secret key from the client. Our security analysis afterwards implies that such blinding technique with homomorphic property can sufficiently prevent adversaries from forging any authenticator of valid messages. Therefore, it will help to make sure our design goal the key updates is as transparent as you possibly can for that client [6]. To Get Rid of the Encrypted Secret Key Verification from the Client, when the client isn't in urgent have to know if the encrypted secret keys downloaded in the OA are correct, we are able to remove his verifying operations making the cloud carry out the verification operations later. Within this situation, we are able to delete the VerEKey formula from your protocol. Whether it holds, then your encrypted secret key should be correct. In this manner, the customer doesn't need to verify the encrypted secret keys immediately after he downloads it in the OA.

Analysis: Within the suggested plan, the important thing update workload is outsourced towards the OA. In comparison, the customer needs to update the key alone in every period of time in plan. Within the designed Sys Setup formula, the OA only holds a preliminary encrypted secret key and also the client holds an understanding key which is often used to decrypt the encrypted secret key. Within the designed Key Update formula, homomorphic property helps make the secret key capable of being updated under encrypted condition and makes verifying the encrypted secret key possible. We assess the performance from the suggested plan through several experiments which are implemented with the aid of the Pairing-Based Cryptography library. The VerESK formula could make the customer look into the validity from the encrypted secret keys immediately. Used, these processes don't take place in the majority of periods of time. They merely take place in time periods once the client must upload new files towards the cloud. In addition, the job for verifying the correctness from the encrypted secret key can fully be carried out by the cloud. We compare the important thing update time on client side between your both schemes. Once the client really wants to upload new files towards the cloud, it must verify the validity from the encrypted secret key in the OA and recover the actual secret key [7]. We demonstrate time from the challenge generation process, the proof generation process, and also the proof verification process with various quantities of checked data blocks. Within our plan, the communicational messages comprise the task message and also the proof message. Once the client really wants to upload new files towards the cloud, it must verify the validity from the encrypted secret key in the OA and recover the actual secret key. We show time of these two processes happened in various periods of time.

4. CONCLUSION:

Existing system doesn't like auditing protocol with verifiable outsourcing of key updates. 3rd party has got the use of see client's secret key without file encryption. One problem we have to resolve would be that the OA should carry out the outsourcing computations for key updates underneath the condition the OA doesn't be aware of real secret key from the client. The customer only must download the encrypted secret key in the OA when uploading new files to cloud. Within this paper, we study regarding how to delegate key updates for cloud storage auditing with

key-exposure resilience. He client can verify the validity from the encrypted secret key as he retrieves it in the TPA. The customer downloads the encrypted secret key.

We demonstrate time from the challenge generation process, the proof generation process, and also the proof verification process with various quantities of checked data blocks. Within our plan, the communicational messages comprise the task message and also the proof message. We advise the very first cloud storage auditing protocol with verifiable outsourcing of key updates. Additionally, the OA only sees the encrypted form of the client's secret key, as the client can further verify the validity from the encrypted secret keys when installing them in the OA. Within this protocol, key updates are outsourced towards the OA and therefore are transparent for that client. We provide the formal security proof and also the performance simulation from the suggested plan.

REFERENCES:

[1] Jia Yu, Kui Ren, Fellow, IEEE, and Cong Wang, Member, IEEE, "Enabling Cloud Storage Auditing With VerifiableOutsourcing of Key Updates", ieee transactions on information forensics and security, vol. 11, no. 6, june 2016.

[2] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[3] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," Int. J. Inf. Secur., vol. 4, no. 4, pp. 277–287, 2005.

[4] C. Guan, K. Ren, F. Zhang, K. Florian, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), 2015, pp. 203–223.

[5] B. Wang, B. Li, and H. Li Oruta, "Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

[6] J. Yu, F. Kong, X. Cheng, R. Hao, and G. Li, "One forward-secure signature scheme using bilinear maps and its applications," Inf. Sci., vol. 279, pp. 60–76, Sep. 2014.

[7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 756–758.

AN OUTSOURCED COMPUTATIONAL IMPLANTED STRATEGY WITH PULL-OFF LEGITIMACY

M Deepika[1] ., K Shravani[2]., G Shruthi [3]., B Kaveri [4] ., K Bindu Sri [5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ mdeepika1 @gmail.com)

2, 3, 4 B.Tech III Year CSE, (16RG1A0540, 16RG1A0533, 16RG1A0556, 16RG1A0551),

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

ABSTRACT: ***The CRA only must hold an arbitrary secret value for the users without having affected the safety of revocable IBE plan. In Search engine optimization and Emura's plan, for every period, each user generates a secret key by multiplying a few of the partial keys, which depends upon the partial keys utilized by ancestors within the hierarchy tree. Another disadvantage is insufficient scalability meaning the KU-CSP must have a secret value for every user. Within the article, we advise a brand new revocable IBE plan having a cloud revocation authority to resolve the 2 shortcomings, namely, the performance is considerably improved and also the CRA holds merely a system secret for the users. Finally, we extend the suggested revocable IBE plan to provide a CRA-aided authentication plan with period-limited rights for managing a lot of various cloud services. In existing system misbehaving/compromised users within an ID-PKS setting is of course elevated. Immediate revocation method employs a delegated semi-reliable an internet-based authority to mitigate the management load from the PKG and assist users to decrypt ciphertext. By experimental results and gratification analysis, our plan is perfect for cellular devices. For security analysis, we've shown our plan is semantically secure against adaptive-ID attacks underneath the decisional bilinear Diffie-Hellman assumption. The suggested present the framework in our revocable IBE plan with CRA and define its security notions to model possible threats and attacks. CRA-aided authentication plan with period-limited rights for managing a lot of various cloud services***

Keywords: Cloud Revocation Authority (CRA), authentication, cloud computing, outsourcing computation, revocation authority..

1. INTRODUCTION:

The PKG is accountable to create each user's private key using the connected ID information. Therefore, no certificate and PKI are needed within the connected cryptographic mechanisms under ID-PKS settings. To enhance the performance, several efficient revocation mechanisms for conventional public key settings happen to be well studied for PKI. An ID-PKS setting includes users along with a reliable 3rd party. The CRA only must hold an arbitrary secret value (master time key) for the users without having affected the safety of revocable IBE plan [1]. In Search engine optimization and Emura's plan, for every period, each user generates a secret key by multiplying a few of the partial keys, which depends upon the partial keys utilized by ancestors within the hierarchy tree. Compared to Li et al.'s plan, the performances of computation and communication are considerably improved. Quite lately, by embedding an outsourcing computation technique into IBE, Li et al. suggested a revocable IBE plan having a key-update cloud company (KU-CSP). However, their plan has two shortcomings. One would be that the computation and communication pricing is greater than previous revocable IBE schemes.

Literature Survey: To be able to alleviate the burden from the PKG in Boneh and Franklin's plan, Boneh et al. suggested another revocation method, known as immediate revocation. with a cloud-aided company, Li et al. introduced an outsourcing computation technique into IBE to propose a revocable IBE plan having a key-update cloud company. Boldyreva et al. suggested a revocable IBE plan to enhance the important thing update efficiency. Their revocable IBE plan is dependent on the idea of the Fuzzy IBE and adopts the entire sub tree approach to decrease the amount of key updates from straight line to logarithmic in the amount of users [2]. Around the contrast, the CRA within our plan holds just one master time key for the users.

2. TRADITIONAL MODEL:

Li et al. introduced an outsourcing computation technique into IBE to propose a revocable IBE plan having a key-update cloud company (KU-CSP). They shifts the important thing-update procedures to some KU-CSP to relieve the load of PKG. Li et al.also used the same technique adopted in Tseng and Tsai's plan, which partitions a user's private key into a name key along with a time update key [3]. The PKG transmits a person the related identity key using a secure funnel. Mean while, the PKG must produce a random secret value for every user and send it towards the KU-CSP. Then your KUCSP generates the

present time update key of the user using the connected time key and transmits it towards the user using a public funnel. Disadvantages of existing system: ID-based file encryption (IBE) enables a sender to secure message directly using a receiver's ID without examining the validation of public key certificate. In existing system misbehaving/compromised users within an ID-PKS setting is of course elevated. Immediate revocation method employs a delegated semi-reliable an internet-based authority to mitigate the management load from the PKG and assist users to decrypt ciphertext. The computation and communication pricing is greater than previous revocable IBE schemes. Another disadvantage is united nations-scalability meaning the KU-CSP must have a time key for every user in order that it will incur the management load.

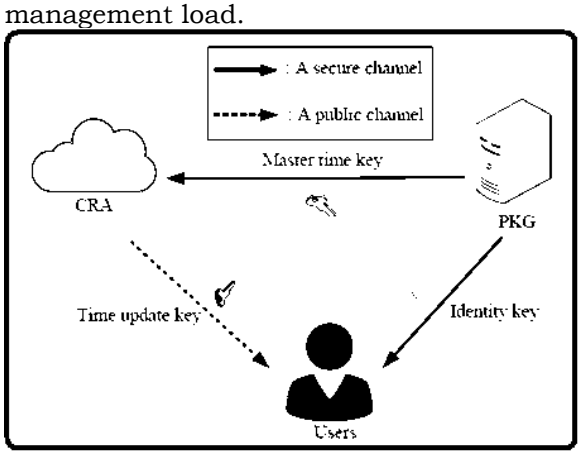


Fig.1.Proposed framework

3. ENHANCED SCHEME:

To be able to solve both united nations-scalability and also the inefficiency in Li et al.'s plan, we advise a brand new revocable IBE plan with cloud revocation authority (CRA). Particularly, each user's private key still includes a name key along with a time update key. We introduce a cloud revocation authority (CRA) to exchange the function from the KU-CSP in Li et al.'s plan. The CRA only must hold an arbitrary secret value (master time key) for the users without having affected the safety of revocable IBE plan. However, their plan requires greater computational and communicational costs than formerly suggested IBE schemes. For that time key update procedure, the KU-CSP in Li et al.'s plan must have a secret value for every user that it is insufficient scalability. Within our revocable IBE plan with CRA, the CRA holds merely a master time answer to carry out the time key update procedures for the users without having affected security. The CRA uses the actual time answer to create the moment update key periodically for every non-revoked user and transmits it towards the user using a public funnel [4]. It's apparent our plan solves the united nations-scalability problem from the KU-CSP. We create a CRA-aided authentication plan with period-limited rights for managing a lot of various cloud services. Benefits of suggested system: The suggested plan offers the benefits of both Tseng and Tsai's revocable IBE plan and Li et al.'s plan. The suggested present the framework in our revocable IBE plan with CRA and define its security notions to model possible threats and attacks. CRA-aided authentication plan with period-limited rights for managing a lot of various cloud services.

Framework: The PKG uses the actual secret key _ to compute the identity key DID from the user with identity ID, and transmits the identity key DID towards the user using a secure funnel. However, the CRA is accountable to create time update keys for the non-revoked users using the master time key. we advise a competent revocable IBE plan with CRA [5]. The plan is built by utilizing bilinear pairings and includes five algorithms. Within the benchmark results, two processors around the Apple Core-2 computer and Htc Desire Mobile Phone HD-A9191 Smartphone are widely-used to simulate the computational costs from the cloud revocation authority (CRA) and mobile users, correspondingly. We construct a formula B to resolve the DBDH trouble with probability. we evaluate the probability the simulation above won't abort. Within the Phases 1 and a pair of, if gold coin =, the simulation continues. Observe that the probability Pr[gold coin =] is decided later. When we put the DBDH problem on every H1 response. we evaluate the probability the simulation above won't abort. Within the Phases 1 and a pair of, if gold coin = , the simulation continues. we define the safety notions for revocable IBE schemes with CRA which include two kinds of the indistinguishability of file encryption, namely, under adaptive ID and selected-plaintext attacks, and under adaptive ID and selected-ciphertext attacks, correspondingly. A person has the capacity to decrypt the ciphertext if she/he offers both identity key and also the legitimate time update key. To revoke a person, the PKG just asks the KU-CSP to prevent issuing the brand new time update key from the user. In the following paragraphs, we suggested a brand new revocable IBE plan having a cloud revocation authority (CRA), where the revocation procedure is conducted

through the CRA to relieve the load from the PKG. This outsourcing computation technique along with other government bodies continues to be used in Li et al.'s revocable IBE plan with KU-CSP. As the amount of user's increases, the burden of key updates turns into a bottleneck for that PKG. A sender utilizes a designated receiver's ID and current period to secure messages as the designated receiver decrypts the ciphertext while using current private key [6]. For constructing such revocable ABE schemes utilizing a public funnel, we might employ exactly the same role from the CRA to result in periodically generating the attribute-time keys for users and send these to users using a public funnel. The actual time secret is substituted for multiple master privilege keys. A CRA having a master privilege key can manage the related privilege to get access to some service server at various periods. A CRA has the capacity to use its master privilege answer to generate and send a period of time-limited privilege answer to a person. Finally, in line with the suggested revocable IBE plan with CRA, we built a CRA aided authentication plan with period-limited rights for managing a lot of various cloud services [7].

4. CONCLUSION:

A CRA having a master privilege key can manage the related privilege to get access to some service server at various periods. A CRA has the capacity to use its master privilege answer to generate and send a period of time-limited privilege answer to a person. A person has the capacity to decrypt the ciphertext if she/he offers both identity key and also the legitimate time update key. To revoke a person, the PKG just asks the KU-CSP to prevent issuing the brand new time update key from the user. Identity-based file encryption (IBE) is really a public key cryptosystem and eliminates the requirements of public key infrastructure (PKI) and certificate administration in conventional public key settings. Because of the lack of PKI, the revocation issue is a vital issue in IBE settings. Several revocable IBE schemes happen to be suggested in regards to this issue.

REFERENCES:

[1] Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang, "Identity-Based Encryption with CloudRevocation Authority and Its Applications", ieee trans. Cloud computing 2016.

[2] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," Proc. Crypto'12, LNCS, vol. 7417 , pp. 199-217, 2012.

[3] Y.-M. Tseng, T.-Y.Wu, and J.-D.Wu, "A pairing-based user authentication scheme for wireless clients with smart cards," Informatica, vol. 19, no. 2, pp. 285-302, 2008.

[4] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Trans. On Computers, vol. 64, no. 2, pp. 425-437, 2015.

[5] D. Boneh, X. Ding, G. Tsudik, and C.-M.Wong, "A Method for fast revocation of public key certificates and security capabilities," Proc. 10th USENIX Security Symp., pp. 297-310. 2001.

[6] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280, 2002.

[7] T. Kitagawa, P. Yang, G. Hanaoka, R. Zhang, K. Matsuura, and H. Imai, "Generic transforms to acquire CCA-security for identity based encryption: The Cases of FOPKC and REACT," Proc. ACISP'06, LNCS, vol. 4058, pp. 348-359, 2006.

HANDLING VOLATILE INTENSIFICATION OF DATA QUANTITY USING ULTRA-LARGE FRACTIONS

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

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ sravanij691@gmail.com)

2, 3, 4 B.Tech III Year CSE, (17RG1A05F2, 17RG1A05F7, 17RG1A05G9),

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

ABSTRACT: ***Existing content-based analysis tools not just cause high complexity and charges, but additionally neglect to effectively handle the huge levels of files. The suggested RTS methodology is implemented like a system middleware that may operate on existing systems, such as the Hadoop file system, using the general file system interface and exploiting correlation property of information. This paper proposes an almost real-time plan, known as RTS, to aid efficient and price-effective searchable data analytics within the cloud. RTS extracts key property information of the given type by means of multidimensional attributes to represent these details in multi-dimensional vectors. An intuitive idea would be to considerably reduce the amount of images to become submitted by discussing just the most representative one instead of all, a minimum of once the cell phone is energy-restricted. RTS take advantage of the VFS operations to aid semantic grouping. We are able to have the data from page cache to help transmit towards the daemon We conduct a genuine-world use situation by which children reported missing within an very crowded atmosphere are identified in due time by analyzing 60 million images using RTS. RTS is made to exploit the correlation property of information by utilizing correlation-aware hashing and manageable flat-structured addressing.***

Keywords: Real Time Search (RTS), cloud storage, data analytics, real-time performance, semantic correlation.

1. INTRODUCTION:

The value or worth of data poor data analytics means the precious understanding hidden within the data that may directly result in economic values/gains running a business intelligence applications or new scientific breakthroughs in scientific applications. searchable data analytics are construed as acquiring data value/worth via queried results, for example locating a valuable record, a correlated process ID, an essential image, a rebuild system log, etc. Because of the unacceptable latency, the staleness of information seriously diminishes the need for data. Data analytics for that cloud typically consume substantial system sources, for example storage, I/O bandwidth, high-performance multiform processors. In some instances, the outcomes of information analytics on stale data can also be misleading, resulting in potential fatal problems [1]. This permits RTS to considerably reduce processing latency of correlated file recognition with acceptably small lack of precision. We discuss the way the RTS methodology could be associated with and accustomed to enhance some storage systems, including Spyglass and Smart Store, in addition to a use situation. Our design alleviates the computation overheads of existing schemes for similarity recognition of files by utilizing locality-sensitive hashing. poor semantic-aware namespace, because of the variable lengths of linked lists, LSH hash tables will probably result in unbalanced loads and unpredictable query performance of vertical addressing. Extensive experimental results demonstrate the efficiency and effectiveness of RTS within the performance enhancements. RTS leverages a Blossom-filter based summarization representation which has the salient options that come with simplicity and simplicity of use. The near-real-time property of RTS enables rapid identification of correlated files and also the significant narrowing from the scope of information to become processed. RTS supports several kinds of data analytics, which may be implemented in existing searchable storage systems. We collect a large and real image set that consists in excess of 60 million images. RTS is further improved by utilizing semantic-aware namespace to supply dynamic and adaptive namespace management for ultra-large storage systems.

2. PREVIOUS APPROACH:

The shared storage back-finish simplifies data management [2]. Spyglass exploits the locality of file namespace and skewed distribution of metadata to map the namespace hierarchy right into a multi-dimensional K-D tree and uses multilevel versioning and partitioning to keep consistency. Mix Apart uses a built-in data caching and scheduling means to fix allow Map Reduce computations to evaluate data stored on enterprise storage systems. The

frontend caching layer enables the neighborhood storage performance needed by data analytics. Glance, a just-in-time sampling-based system, can offer accurate solutions for aggregate and top-k queries without prior understanding. Disadvantages of existing system: Existing content-based analysis tools not just cause high complexity and charges, but additionally neglect to effectively handle the huge levels of files. Our prime complexity routinely results in very slow processing operations and incredibly high and frequently unacceptable latency. Because of the unacceptable latency, the staleness of information seriously diminishes the need for data. Existing methods to unstructured data search and analytics depend on either system-based chunks of information files. Because of the lengthy latency incurred in information systems and also the resulting data staleness, the worthOrreally worth of information becomes reduced and finally nullified [3].

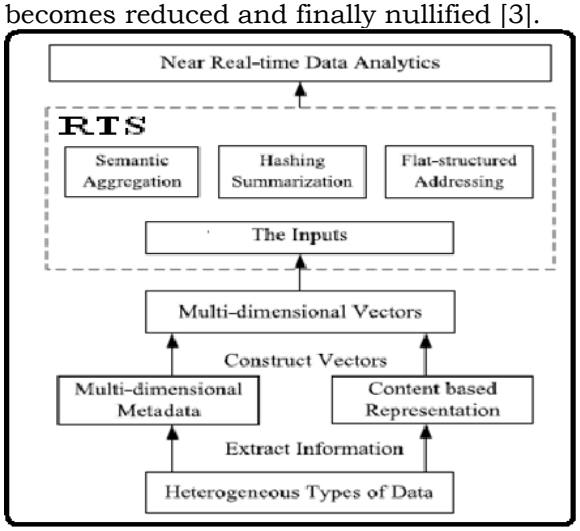


Fig.1.Proposed framework

3. FINE-GRAINED METHOD:

We advise a singular near-real-time methodology for analyzing massive data, known as RTS, having a design objective of efficiently processing such data inside a real-time manner. Poor this paper, searchable data analytics are construed as acquiring data value/worth via queried results, for example locating a valuable record, a correlated processID, an essential image, a rebuild system log, etc. The important thing idea behind RTS would be to explore and exploit the correlation property within using one of datasets via improved correlation aware hashing and flat-structured addressing to considerably lessen the processing latency of parallel queries, while incurring acceptably small lack of precision [4]. The approximate plan legitimate-time performance continues to be broadly recognized in system design and-finish computing. Essentially, RTS goes past the straightforward mixture of existing strategies to offer efficient data analytics via considerably elevated processing speed. Through study regarding the RTS methodology, we aim to help make the following contributions for near real-time data analytics.

Methodology: The ensuing frequent disk I/Os and network transmissions further aggravate the execution performance. Second, some applications encounter periodic system crashes, which results in re-computation that substantially lengthens the latency. Actually, mixing forensic image data from personal and professional sources has labored formerly too. Most file systems or their traces range from the multi-dimensional attributes to aid real-time situation. We consult with the concerning the reasons. The primary reasons, based on the researchers, are twofold. Affinity poor these studies refers back to the semantic correlation produced from multi-dimensional file attributes which include but aren't restricted to temporal or spatial locality [5]. RTS is shown to become a helpful tool in supporting near real-time processing of real-world data analytics applications. the correlation aware hashing would be to find out the correlated files through the hash-computing manner, for example locality-sensitive hashing. RTS extracts key property information of the given type by means of multidimensional attributes to represent these details in multi-dimensional vectors. One salient feature would be that the namespace is flat without hierarchy. To be able to precisely represent the namespace, RTS utilizes multi-dimensional, instead of single-dimensional, attributes to recognize semantic correlations. Existing systems could be enhanced to attain better performance.

Methods and Framework: There is a lot of similar multimedia images within the cloud. We advise to utilize a crowd-based aid, i.e., personal images that may be freely utilized, to recognize useful clues. e can rapidly have the clues suggesting if the missing child had ever made an appearance round the Big Ben. High-resolution cameras offer high picture quality and multiple angles. according to our observations and real-world reports, users have become more and more prepared to share their sightseeing images because of the shared interests and also the easy internet access. Within the SA module, RTS employs locality sensitive hashing to capture correlated

features that identify similar images. RTS includes two primary functional modules, i.e., big information systems and semantic correlation analysis. The area-efficient representation enables the primary memory to contain more features. Generally, two similar images imply they contain many identical features. To do accurate and reliable matching between different views of the object or scene that characterize similar images, we extract distinctive invariant features from images [6]. An incorrect positive implies that different images are put in to the same bucket. An incorrect negative implies that similar images are put into different buckets. Unlike conventional directory based hierarchy, RTS take advantage of the VFS operations to aid semantic grouping. We are able to have the data from page cache to help transmit towards the daemon. We implemented a RTS prototype from the use situation on the 256-node cluster. RTS hence leverages the verification and responses from users to assist determine the query precision. This paper proposes an almost real-time plan, known as RTS, to aid efficient and price-effective searchable data analytics within the cloud. Among the key parameters may be the metric R that regulates the way of measuring approximate membership. The LSH-based structures could work well if R is roughly comparable to the space between your queried point q and it is nearest neighbors [7]. RTS leverages its near-duplicate identification method to considerably reduce the quantity of images to become transmitted. The query latency of RTS is a lot shorter than the other schemes and stays roughly. Since RNPE leverages simple but error-prone tags to recognize similar images, her cheapest precision. PCA-SIFT, however, uses compact feature vectors and performs dimensionality reduction.

4. CONCLUSION:

The concept behind RTS would be to explore and exploit the semantic correlation within using one of datasets via correlation-aware hashing and manageable flat-structured addressing to considerably lessen the processing latency, while incurring acceptably small data loss-search precision. This paper proposes an almost real-time plan, known as RTS, to aid efficient and price-effective searchable data analytics within the cloud. Our design alleviates the computation overheads of existing schemes for similarity recognition of files by utilizing locality-sensitive hashing. poor semantic-aware namespace, because of the variable lengths of linked lists, LSH hash tables will probably result in unbalanced loads and unpredictable query performance of vertical addressing.

REFERENCES:

[1] Y. Ke and R. Sukthankar, "PCA-SIFT: A more distinctive representation for local image descriptors," in Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2004, pp. 506–513.

[2] S. Kavalanekar, B. Worthington, Q. Zhang, and V. Sharda, "Characterization of storage workload traces from production Windows servers," in Proc. IEEE Int. Symp. Workload Characterization, 2008, pp. 119–128.

[3] X. Tan and B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting conditions," IEEE Trans. Image Process., vol. 19, no. 6, pp. 1635–1650, Jun. 2010.

[4] S. Lakshminarasimhan, J. Jenkins, I. Arkatkar, Z. Gong, H. Kolla, S.-H. Ku, S. Ethier, J. Chen, C. S. Chang, S. Klasky, R. Latham, R. Ross, and N. F. Samatova, "ISABELA-QA: Query-driven analytics with ISABELA-compressed extreme-scale scientific data," in Proc. Int. Conf. High Perform. Comput., Netw., Storage Anal., 2011, pp. 1–11.

[5] Yu Hua, Senior Member, IEEE, Hong Jiang, Fellow, IEEE, and Dan Feng, Member, IEEE, "Real-Time Semantic Search Using ApproximateMethodology for Large-Scale Storage Systems", ieee transactions on parallel and distributed systems, vol. 27, no. 4, april 2016.

[6] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[7] A. Andoni and P. Indyk, "Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions," Commun. ACM, vol. 51, no. 1, pp. 117–122, 2008.

INTRODUCING CROSS-MODEL NETWORK FOR ENCODING EXPLICIT/IMPLICIT RELEVANCE

S Sagarika[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 (✉ sagarika.547@gmail.com)

2, 3, 4, 5 B.Tech III Year CSE, (15RG1A0527, 15RG1A0513, 15RG1A0534, 15RG1A0541),

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

ABSTRACT: ***The primary objective of the suggested model would be to perform mix-modal ranking, which is different from those of DeepWalk that aims to understanding the latent representation for classifying the static people of the social networking. Within this paper, we treat the press data like a large click graph, by which vertices are images/text queries and edges indicate the clicks between a pictures along with a query. By modeling the multimodal click graph with a stream of short random walks and adapting techniques of deep neural systems, we produce an finish-to-finish solution, named Multimodal Random Walk Neural Network that can take a multimodal click graph as input to understand the most popular latent representation of text and imagery. The learned space is restricted to become a low dimensional continuous space because the intrinsic dimensionality of the semantic space is generally reduced compared to original feature space. our prime-quality click information is harvested through the collective intelligence from the users without any extra effort in the users. The disadvantage from the existing model is it cannot be relevant to the brand new emerging queries or images. The suggested model not just captures better semantics from the training queries and pictures, but additionally generalizes towards the unseen queries and pictures better. The mapped representation also needs to encode the implicit connections between your vertices within the click graph. When employed for mix-modal retrieval, realizing the click graph may very well be not just text-query-image ranking examples.***

Keywords: Deep learning, cross-media search, click log, latent representation, image accuracy MRWNN..

1. INTRODUCTION:

In multimedia information retrieval, most classic approaches have a tendency to represent different modalities of media within the same feature space. Using the click data collected in the users' searching behavior, existing approaches take each one-to-one paired data or ranking examples as training examples, that do not take advantage of the press data, specially the implicit connections one of the data objects [1]. Therefore, the press data has attracted a lot of research dedicated to the introduction of algorithms for learning an ideal common representation of various modalities. By optimizing both truncated random walk loss along with the distance between your social representation and also the internal representation from the vertices, the social representations from the vertices and also the parameters from the deep neural systems are learned. Another type of the approaches is dependent on the strategy of understanding how to rank, which model the press data as some mix-modal ranking examples. When employed for mix-modal retrieval, MRW-NN simply outputs the latent representation of queries and pictures through the deep neural systems. The learned space is restricted to become a low dimensional continuous space because the intrinsic dimensionality of the semantic space is generally reduced compared to original feature space. our prime-quality click information is harvested through the collective intelligence from the users without any extra effort in the users To lessen these gaps, an average strategy is to map the multimodal data right into a common semantic feature space, and so the retrieval process could be conducted within the recently mapped space [2]. Therefore, the query-image pairs may very well be "soft" relevance judgments to assist bridge the heterogeneity gap. By constraining the space between your latent representation from the vertices as well as their neural network output, robust high-level latent representation is learned.

2. BASIC MODEL:

The scalability of incorporating new semantic concepts into the semantic space is studied, which enables the updated embedding function to be relevant to dynamic image repositories. Craswell et al. propose a Markov random walk model to a sizable click log for locating relevant documents, including those that as-yet unlocked for any query, without analyzing the query content or image content. Rasiwasiaet al. presents that modeling the correlations between modalities is more effective in feature spaces with greater amounts of abstraction [3]. Disadvantages of existing system: These techniques derive from the strategy of understanding how to rank and go ahead and take ranking examples because

the pair wise (or list wise) input to optimize a particular ranking loss. PAMIR may be the first make an effort to address the issue of ranking images by text queries. The issue of ranking images by text queries. PAMIR formulates the mix-modal retrieval problem in ways much like those of Rank SVM and derives a competent training procedure by adapting the Passive-Aggressive formula.

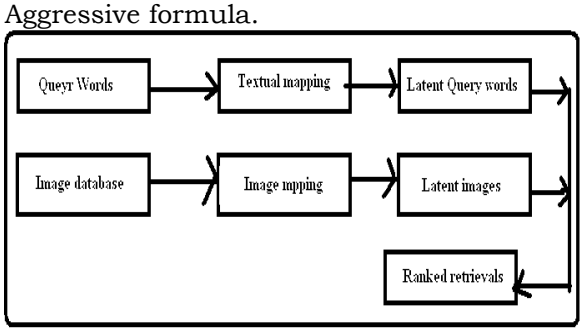


Fig.1.Proposed system framework

3. DYNAMIC ARCHITECTURE:

By optimizing both truncated random walk loss along with the distance between your social representation and also the internal representation from the vertices, the social representations from the vertices and also the parameters from the deep neural systems are learned [4]. Through the minimization from the random walk error and also the regularization penalty in the creation of the modal-specific neural systems, the learned model is able not just to represent the specific connections and also the implicit connections from the vertices within the click graph with low-dimensional continuous vectors, but additionally to map the unseen queries and pictures towards the latent subspace to aid mix-modal retrieval. Thus the suggested model not just captures better semantics from the training queries and pictures, but additionally generalizes towards the unseen queries and pictures better. The suggested MRW-NN model could be integrated using the deep structure of those methods, although it remains a wide open question within our further work whether there's a particular (and) deep structure for modeling the written text queries and also the images within the click graph. The suggested MRW-NN, CMRNN takes two modality-specific neural systems for mapping the queries and also the images right into a common subspace, although it optimizes the list wise ranking lack of the mix-modal ranking examples. We consider learning a multimodal representation in the outlook during encoding the specificOrimplied relevance relationship between your vertices within the click graph. By minimizing both truncated random walk loss along with the distance between your learned representation of vertices as well as their corresponding deep neural network output, the suggested model that is named multimodal random walk neural network (MRW-NN) does apply not only to learn robust representation from the existing multimodal data within the click graph, but additionally cope with the unseen queries and pictures to aid mix modal retrieval [5]. Benefits of suggested system: The suggested model not just captures better semantics from the training queries and pictures, but additionally generalizes towards the unseen queries and pictures better. When employed for mix-modal retrieval, Realizing the click graph may very well be not just text-query-image ranking examples but additionally image-query-text ranking examples, Bi-CMSRM suggested intakes bi-directional ranking examples into consideration, so that two directions of retrieval are enhanced concurrently, yielding a much better representation for multimodal data. First suggests using random walks to understand latent representation around the social community graph. Within this work, we constrain ourselves to understand the latent representation from the multimodal click graph. Click Aware: The greater the specific clicks from a query as well as an image, the closer their latent representation ought to be. Generalization Aptitude: It's inadequate to understand latent representation for that present people from the click graph only and also the suggested modal will be able to perform mix-modal ranking later on.

Framework: The suggested method MRW-NN learns an over-all multimodal representation in the training click graph meaning it maps the two kinds of multimodal data in to the same common space where the mix-modal retrieval can be carried out. Our jobs are carefully associated with DeepWalk which first suggests using random walks to understand latent representation around the social community graph. However, deep neural systems (DNNs) that become familiar with a transformation of the low-level representation to some high-level representation have proven their effective capability to the duties of learning multimodal representation. The actual assumption of CCL would be that the greater the press number, the smaller sized the space between your query and also the image within the latent space. The aim of PAMIR and DeViSE would be to minimize the typical quantity of the inversions in ranking

that's, the greater clicked images ought to be rated greater compared to less clicked ones. We aim to perform mix-modal ranking within the new images and queries that aren't active in the training click graph. We've shown the potency of the learned representation through the suggested method MRW-NN and proven its better than the comparative methods on mix-modal retrieval on the large-scale click log dataset. The mapped representation also needs to encode the implicit connections between your vertices within the click graph. Most significantly, the mapping functions should generalize for that unseen images and emerging queries well [6]. The DCNN model includes several convolutional filtering, local contrast normalization and max-pooling layers, adopted by a number of fully connected neural network layers. we advise an finish-to-finish learning solution and formulate our objective within the look at well-known "empirical risk regularization" framework. Inspired through the DeepWalk model, the representation from the vertices from the click graph is learned from the stream of truncated random walks, using optimization techniques initially created for language modeling. The suggested model is needed to maximize the prospect of observing only vertices appearing right side from the given vertex within the random walk, instead of that appearing to each side within the DeepWalk model. we consider analyzing the information from the vertices. Within this work, we've presented a brand new method of learning latent representation from the multimodal data from the click graph. To resolve the regularized optimization, the overall optimization process of MRW-NN alternates between two steps, one generating random walks and yet another updating the parameters. To use the computation abilities efficiently, we make use of the data parallelism training. Within this work, each word is learned to become connected having a low-dimensional continuous vector within the word look-up table [7]. One easy method to investigate learned representation is to locate the nearest words for any specific word. The press count between a pictures along with a totally summed from various users at different occasions. Some parameters ought to be fixed throughout the training procedure such as the dimensionality from the latent space d, while some could be adjusted.

4. CONCLUSION:

The suggested model not just captures better semantics from the training queries and pictures, but additionally generalizes towards the unseen queries and pictures better. When employed for mix-modal retrieval, the mapped representation also needs to encode the implicit connections between your vertices within the click graph. Most significantly, the mapping functions should generalize for that unseen images and emerging queries well. We assess the latent representation learned by MRW-NN on the public large-scale click log data set Clickture and additional reveal that MRW-NN achieves far better cross modal retrieval performance around the unseen queries/images compared to other condition-of-the-art methods. The suggested MRW-NN model could be integrated using the deep structure of those methods, although it remains a wide open question within our further work whether there's a particular (and) deep structure for modeling the written text queries and also the images within the click graph.

REFERENCES:

[1] Fei Wu, Xinyan Lu, Jun Song, Shuicheng Yan, Senior Member, IEEE, Zhongfei (Mark) Zhang,Yong Rui, Fellow, IEEE, and Yueting Zhuang, "Learning of Multimodal Representations WithRandom Walks on the Click Graph", ieee transactions on image processing, vol. 25, no. 2, february 2016.

[2] X. Lu, F. Wu, S. Tang, Z. Zhang, X. He, and Y. Zhuang, "A low rank structural large margin method for cross-modal ranking," in Proc. 36th Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retr., 2013, pp. 433–442.

[3] M. Belkin and P. Niyogi, "Laplacian eigenmaps for dimensionality reduction and data representation," Neural Comput., vol. 15, no. 6, pp. 1373–1396, 2003.

[4] G. Smith, C. Brien, H. Ashman, "Evaluating implicit judgments from image searchclickthrough data," J. Amer. Soc. Inf. Sci. Technol., vol. 63, no. 12, pp. 2451–2462, 2012.

[5] Y. Yang, Y.-T. Zhuang, F. Wu, and Y.-H. Pan, "Harmonizing hierarchical manifolds for multimedia document semantics understanding and crossmedia retrieval," IEEE Trans. Multimedia, vol. 10, no. 3, pp. 437–446, Apr. 2008.

[6] D. R. Hardoon, S. Szedmak, and J. Shawe-Taylor, "Canonical correlation analysis: An overview with application to learning methods," Neural Comput., vol. 16, no. 12, pp. 2639–2664, Dec. 2004.

LOWERING AMBIGUITY DISPENSATION COSTS USING LEAKAGE DETERRENCE SCHEME

A Brahmareddy[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 (✉ brahmareddy475@gmail.com)

2, 3, 4, 5 B.Tech III Year CSE, (16RG1A0577, 16RG1A0583, 16RG1A0599, 17RG1A0501),

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

ABSTRACT: ***More concretely, previous searchable encryptions particularly handling order comparisons or Order-Preserving File encryption can be extended and leveraged to allow axis-parallel rectangular range explore spatial data. an information analyzer can study social achieve ability according to countless users' location check-ins by evaluating multiple models of circular range queries. While the majority of the searchable file encryption schemes concentrate on common SQL queries, for example keyword queries and Boolean queries, couple of research has particularly investigated geometric range search over encrypted spatial data. Our major contributions is the fact that our design is really a general approach, which could support various kinds of geometric range queries. None of those previous works have particularly studied geometric range queries that are expressed as non-axis-parallel rectangles or triangles. With rapid developments of social systems, Location-Based Services and traveling with a laptop, the quantity of data people create everyday keeps growing dramatically. It's no longer easy or perhaps lucrative for businesses keep a lot of data in your area. More to the point, there still lacks an over-all approach, which could flexibly and safely support various kinds of geometric range queries over encrypted spatial data no matter their specific geometric shapes. Our design has great potential for use and implemented in wide applications, for example Location-Based Services and spatial databases, where using sensitive spatial data having a dependence on strong privacy guarantee is required.***

Keywords: SQL queries, Geometric range search, spatial data, encrypted data, and social nets..

1. INTRODUCTION:

The objective of geometric range explore a spatial dataset would be to retrieve points which are in the particular geometric range. We formally define and prove the safety in our plan within distinguish ability under selective selected-plaintext attacks, and demonstrate the performance in our plan with experiments inside a real cloud platform. Within this paper, we advise a symmetric-key probabilistic Geometric Range Searchable File encryption [1]. With this plan, a semi-honest cloud server can verify whether a place is in the geometric range over encrypted spatial datasets. Our design is really a general approach, which could safely support various kinds of geometric range queries on encrypted spatial data no matter their geometric shapes. Geometric range search is really a fundamental primitive for spatial data analysis in SQL and NoSQL databases. Its extensive applications in location-based services, cad, and computational geometry. Observe that establishing a minimal bounding axis-parallel rectangle for just about any geometric object, e.g., a triangular, a circle or perhaps a non-axis-parallel rectangle, could be an alternate choice for individuals preceding schemes to construct an over-all solution supporting various kinds of geometric range queries. a few of the recent works, private closeness testing, which will help two users to safely verify whether one user is in the circle of some other user based their private locations, will also be constructed from Secure Multi-party Computation [2]. Because of the dramatic rise in data size, it's important for organizations and companies to delegate their spatial data sets to 3rd-party cloud services to be able to reduce storage and query processing costs, but, meanwhile, using the commitment of no privacy leakage towards the 3rd party. Therefore, it's a demanding task to construct an over-all geometric range searchable file encryption, which could perform various kinds of range queries.

2. CLASSICAL MODEL:

Wang et al. suggested a singular plan to particularly perform circular range queries on encrypted data by leveraging some concentric circles. Some previous searchable encryptions handling order comparisons can basically manage axis parallel rectangular range explore encrypted spatial data. Similarly, Order-Preserving File encryption, that has less strong privacy guarantee than searchable file encryption, can also be capable of singing axis-parallel rectangular range search with trivial extensions. Ghinita and Rughinis particularly leveraged certain Functional File encryption with hierarchical encoding to efficiently operate axis-parallel rectangular range explore encrypted spatial data in the use of mobile users monitoring [3]. Searchable file

encryption is really a method to perform significant queries on encrypted data without revealing privacy. However, geometric range explore spatial data is not fully investigated nor based on existing searchable file encryption schemes. Within this paper, we design a symmetric-key searchable file encryption plan that may support geometric range queries on encrypted spatial data. Disadvantages of existing system: The majority of the searchable file encryption schemes concentrate on common SQL queries, for example keyword queries and Boolean queries, couple of research has particularly investigated geometric range search over encrypted spatial data. Inevitably introduces obstacles when it comes to search functionalities over encrypted data.

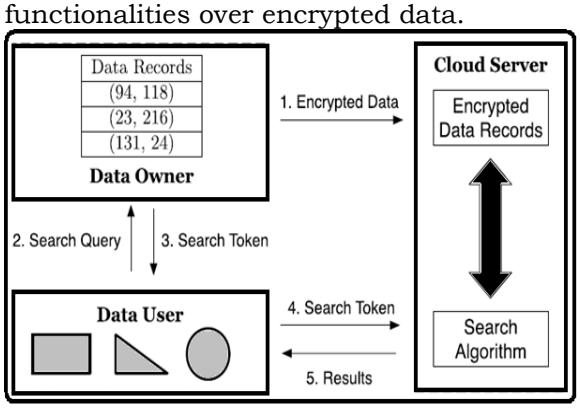


Fig.1.Proposed system framework

3. IMPROVED METHOD:

Within this paper, we advise a symmetric-key probabilistic Geometric Range Searchable File encryption. With this plan, a semi-honest cloud server can verify whether a place is in the geometric range over encrypted spatial datasets. Particularly, our option would be independent using the form of a geometrical range query. Using the additional utilization of R-trees, our plan has the capacity to achieve faster-than-straight line search complexity regarding to the amount of points inside a dataset [4]. The safety in our plan is formally defined and examined within distinguish ability under Selective Selected-Plaintext Attacks. Informally, except understanding the necessary Boolean Google listing of the geometric range search, the semi-honest cloud server can't reveal any personal data about data or queries. Our primary contributions are summarized the following: Additionally, our search process is non-interactive on encrypted data. When it comes to search complexity, our baseline plan incurs straight line complexity, and it is advanced version realizes quicker than-straight line search by integrating with tree structures. In addition, our design isn't just appropriate for geometric range queries, but additionally suitable for other regular kinds of geometric queries, for example intersection queries and point enclosure queries, over encrypted spatial data. Benefits of suggested system: The safety in our plan is formally defined and examined within distinguish ability under Selective Selected-Plaintext Attacks.

Fundamental Statements: The objective of a geometrical range totally to retrieve points which are within the geometric range. we assume the information we handle within this paper are positive integers. To be able to flexibly manage different geometric range queries, our primary design methodology within this paper would be to preprocess each kind of geometric range queries to some same form within the plaintext domain. This Fundamental plan is straightforward and efficient [5]. Regrettably, it just provides limited privacy protection. The preceding description of the symmetric-key GRSE is probabilistic automatically, which is deterministic if both Enc and GenToken are deterministic. We practice a general method of safely search encrypted spatial data with geometric range queries. The main kinds of geometric objects we look into this paper include rectangles, circles and triangles. Since all these geometric object represents a shut area. Stated differently, you will find false positives but no false negatives. Other intriguing and important rentals are that, the Blossom filter from the intersection of two sets could be roughly calculated with bitwise-And processes. When compared to deterministic one, this probabilistic plan can offer both data privacy and query privacy under IND-SCPA. The next symmetric-key lattice-based Functional File encryption enabling inner products can be simply embedded to the design to help boost efficiency by replacing SSW because the foundation. To the very best of our understanding, SSW may be the condition-of-the-art Functional File encryption [6]. Therefore, we describe another way, named Trick-1, to ensure whether a component is incorporated in the group of a Blossom filter, where Trick-1 is dependent on the qualities from the intersection of two Blossom filters. Thinking about the operations of adding elements right into a Blossom filter in plaintext domain tend to be quicker than those utilized in file encryption with SSW. One of the leading benefits of achieving non-interactive evaluation on encrypted data in searchable file encryption is the fact that, the customer doesn't have to become online constantly or spend high

communication overheads during query processing.

Extensions: One method to enhance the search complexity is by using tree structures. The fundamental concept of building an R-tree would be to group nearby points (or rectangles) and represent them right into a minimal bounding box within the next greater degree of the tree. To secure a place, an information owner still uses exactly the same way as before to secure a rectangle of every non-leaf node, an information owner enumerates all of the possible points inside this rectangle within the plaintext domain. To mitigate this, we are able to always minimize the particular false positive odds at these non-leaf nodes by growing the size of Blossom filters. Therefore, proper parameters ought to be taken while using the tree-based approach, to ensure that a great tradeoff between false positive odds at non-leaf nodes and also the total search time is possible [7]. The objective of point enclosure search would be to retrieve geometric objects which contain the query point. Our design has great potential for use and implemented in wide applications, for example Location-Based Services and spatial databases, where using sensitive spatial data having a dependence on strong privacy guarantee is required. Furthermore, we leverage the pre-processing model in PBC to improve the performance of pairing operations. Once we mentioned in the last section, while using the tree-based approach, a tradeoff exists between false positives at non-leaf nodes and also the total search time. The parameter dominates the efficiency of search time per point is the size of a Blossom filter m, that is basically the vector period of SSW. Therefore, a little tradeoff on FPP at non-leaf nodes within the tree can considerably enhance the actual search time.

4. CONCLUSION:

We present a symmetric-key probabilistic Geometric Range Searchable File encryption, and formally define and prove its security within distinguish ability under Selective Selected-Plaintext Attacks (IND-SCPA). To secure a place, an information owner still uses exactly the same way as before to secure a rectangle of every non-leaf node, an information owner enumerates all of the possible points inside this rectangle within the plaintext domain. Using the additional utilization of R-trees, our plan has the capacity to achieve faster-than-straight line search complexity regarding to the amount of points inside a dataset. we formally present the phrase a symmetric-key Geometric Range Searchable File encryption. More particularly, with the ability to indicate a component is either certainly away from the set or even within the set. Our design is really a general approach, which could safely support various kinds of geometric range queries on encrypted spatial data no matter their geometric shapes.

REFERENCES:

[1] Boyang Wang, Student Member, IEEE, Ming Li, Member, IEEE, and Haitao Wang, "Geometric Range Search on Encrypted Spatial Data", ieee transactions on information forensics and security, vol. 11, no. 4, april 2016.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD, 2004, pp. 563–574.

[3] C. Shahabi, L. Fan, L. Nocera, L. Xiong, and M. Li, "Privacy-preserving inference of social relationships from location data: A vision paper," in Proc. ACM SIGSPATIAL GIS, 2015, pp. 1–4.

[4] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. EUROCRYPT, 2008, pp. 146–162.

[5] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in Proc. Workshop New Secur. Paradigms, 2001, pp. 13–22.

[6] B. Wang, M. Li, S. S. M. Chow, and H. Li, "A tale of two clouds: Computing on data encrypted under multiple keys," in Proc. IEEE CNS, Oct. 2014, pp. 337–345.

[7] S. Agrawal, D. M. Freeman, and V. Vaikuntanathan, "Functional encryption for inner product predicates from learning with errors," in Proc. ASIACRYPT, 2011, pp. 21–40.

PRIVACY LEAK PREVENTIVE AND URL SHORTENING SCHEME FOR SHORT MESSAGE TRANSMISSION

T Venkata Seshu Kiran[1]., R Likitha[2]., S Likhitha[3]., M Amrutha[4]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ seshukiran04@gmail.com)

2, 3, 4 B.Tech III Year CSE, (16RG1A0585, 16RG1A0588, 16RG1A0563),

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

ABSTRACT: Within this paper, we advise novel attack means of inferring whether a particular user visited certain shortened URLs on Twitter. Our attacks depend around the mixture of openly available information: click analytics from URL shortening services and metadata from Twitter. To do the 2nd attack, we create monitoring accounts that monitor messages all followings of target users to gather all shortened URLs the target users may click. Then we monitor the press analytics of individuals shortened URLs and do a comparison using the metadata from the target user. Previous research has considered attack techniques that create privacy leaks in social systems, for example inferring private attributes and de-anonymizing users. Evaluation results reveal that our attacks can effectively infer the press information rich in precision and occasional overhead. We advise novel attack strategies to see whether a particular user clicks certain shortened URLs on Twitter.

Keywords: Twitter, URL Shortening Service, Privacy leak, Inference.

1. INTRODUCTION:

Twitter enables users to publish as much as 140-character tweets that contains only texts. Therefore, when users wish to share complicated information. However, we identify an easy inference attack that may estimate individual visitors in the aggregated, public click analytics using public metadata supplied by Twitter. Twitter is a well-liked online social networking service for discussing short messages (tweets) among buddies. Its users frequently use URL shortening services that offer (i) a brief alias of the lengthy URL for discussing it via tweets and (ii) public click analytics of shortened URLs. The primary benefit of the preceding inference attack within the conventional browser history stealing attacks is it only demands public information [1]. The traditional browser history stealing attacks depend on personal data. Within this paper, we advise novel attack means of inferring whether a particular user visited certain shortened URLs on Twitter. We advise novel attack strategies to see whether a particular user clicks certain shortened URLs on Twitter. To the very best of our understanding, this is actually the first study that infers URL visiting history on Twitter [2].

2. TRADITIONAL MODEL:

Some researchers propose attack techniques to steal browsing history using user interactions and side-channels. Weinberg et al. exploit CAPTCHA to trick users and also to induce user's interaction. Additionally they make use of a webcam to identify the sunshine from the screen reflected in the user's face, that you can use to differentiate the colors of visited from individuals of unvisited links. He et al. and Lindamoodet al. develop a Bayesian network to calculate undisclosed personal attributes. Zheleva and Getoor show how an assailant can exploit a combination of public and private data to calculate private features of a target user. Similarly, Mnislove et al. infer the features of a target user using a mixture of features of the user's buddies along with other users who're loosely (in a roundabout way) attached to the target user [3]. Unlike the traditional browser history stealing attacks, our attacks only demand openly available information supplied by Twitter and URL shortening services. Evaluation results reveal that our attack can compromise Twitter users' privacy rich in precision.

Calandrino et al. propose algorithms inferring customer's transactions within the recommender systems, for example Amazon . com and Hunch. Disadvantages of existing system: Previous research has considered attack techniques that create privacy leaks in social systems, for example inferring private attributes and de-anonymizing users.

Many of them combine public information from the 3 different datasets to infer hidden information. Need complicated techniques or assumptions.

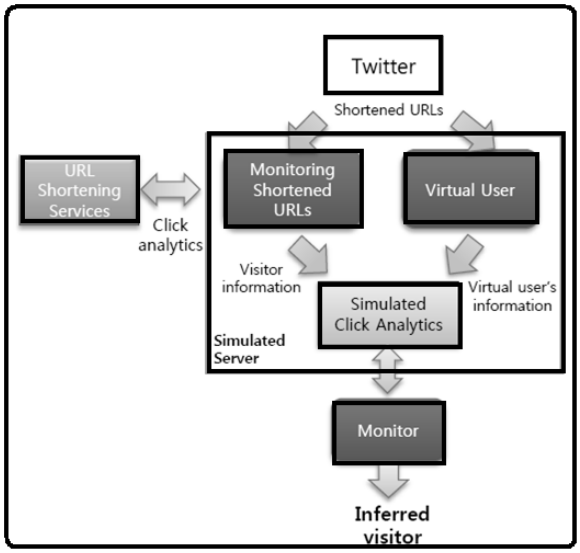


Fig.1.Proposed architecture

3. ENHANCED SCHEME:

The aim of the attacks would be to know which URLs are visited by target users. We introduce two different attack methods:(i) a panic attack to understand who click the URLs updated by target users and (ii) a panic attack to understand which URLs are visited by target users. To do the very first attack, we discover numerous Twitter users who frequently distribute shortened URLs, and investigate click analytics from the distributed shortened URLs and also the metadata from the supporters from the Twitter users. The general public click analytics is supplied within an aggregated form to preserve the privacy of person users. Within this paper, we advise practical attack techniques inferring who clicks which shortened URLs on Twitter while using mixture of public information: Twitter metadata and public click analytics.

To do the 2nd attack, we create monitoring accounts that monitor messages all followings of target users to gather all shortened URLs the target users may click. Then we monitor the press analytics of individuals shortened URLs and do a comparison using the metadata from the target user. In addition, we advise a sophisticated attack approach to reduce attack overhead while growing inference precision while using time type of target users, representing once the target users frequently use Twitter. Benefits of suggested system: Evaluation results reveal that our attacks can effectively infer the press information rich in precision and occasional overhead [4]. We advise novel attack strategies to see whether a particular user clicks certain shortened URLs on Twitter.

To the very best of our understanding, this is actually the first study that infers URL visiting history on Twitter. We simply use public information supplied by URL shortening services and Twitter (i.e., click analytics and Twitter metadata). We see whether a target user visits a shortened URL by correlating the openly available information. Our approach doesn't need complicated techniques or assumptions for example script injection, phishing, adware and spyware invasion, or DNS monitoring. All we want is openly available information. We further decrease attack overhead while growing precision by thinking about target users' time models. It may boost the functionality in our attacks to ensure that we demand immediate countermeasures.

Shortening of URL: URL shortening services reduce the size of URLs by supplying short aliases of URLs to requesters and redirecting later people to the initial URLs. In comparison, goo.gl records only "t.co" within the Referrers field. When we make use of the information supplied by bit.ly, we are able to determine the precise Link to the tweet that contains the clicked shortened URL.

The fundamental concept of our attack is recording instant alterations in the general public click analytics of shortened URLs by periodically monitoring it and matching the moment changes using the details about target users to infer whether our target users result in the changes. The press analytics of goo.gl only records the hostname from the referrer site. If your customer originates from Twitter, "t.co" or "twitter.com" is recorded within the Referrers field. Within the periodic monitoring, figuring out the perfect query interval is essential, which depends upon the range of the options of supporters. Oftentimes, Twitter users complete the place field using their city or place name. We are able to determine the user's country by searching GeoNames using the information within the location field from the user's Twitter profile. GeoNames returns the nation code that matches looking keywords [5]. Although Twitter doesn't provide information such as this about its users, it will record the specific application which was accustomed to publish a tweet. The definite methods to exactly evaluate our attacks are (i) asking the prospective users whether or not they really visited the shortened URLs or (ii) monitoring their browsing activities by utilizing logging software. We can't test all kinds of

Twitter users since they're too diverse, therefore we restrict the amount of user types for the experiment. Whether our bodies can properly recognize the clicks of virtual users depends upon the distinctiveness from the virtual users against other supporters of posting users. In comparison, false positives are possible because some Twitter users have a similar information because the virtual users. Consequently, our bodies may incorrectly guess virtual users since it misjudges the supporters because the virtual user. We anticipate seeing low precision with iPhone and Android users because of the many users on individual's platforms. The general precision in our attack product is lower with bit.ly than by using goo.gl, because goo.gl offers four kinds of information within the click analytics. If not one other user has got the same information because the target user, our bodies can properly infer the prospective user whatever the quantity of the posting user's supporters.

Real-time Inference Attacks: The machine blogs about the details about the customer using the known information the prospective user. If both information match, it infers the target user clicks the shortened URL. First, it might contain URLs visited by other Twitter users who have a similar features because the target user. Second, the ultimate candidate set might not incorporate a shortened URL visited through the target user once the target user clicks the shortened URL in various country and/or platform [6].

The ultimate candidate user set may contains wrong candidate users since the target user has numerous supporters who share exactly the same features. However, it's possible the target user changes his Smartphone or travels to overseas. In Attack II, we decide target users who frequently update shortened URLs for acquiring enough experimental data. We think that Twitter users include URLs within their tweets and favorite tweets with URLs only if they formerly go to the URLs. To explain, guess that our bodies infers that the Twitter user A visits a shortened URL U. A tweet that contains a shortened URL could be read by users who aren't supporters from the user who published the tweet, via retweets or any other channels, so non-supporters may click the shortened URL. We crawled tweets which were over the age of eventually because we would have liked to gather tweets which had lots of time to be retweeted.

Advanced Inference Attack: we introduce a sophisticated inference attack that decreases attack overhead while growing inference precision. Within this paper, we suggested inference attacks to infer which shortened URLs visited with a target user. All the details necessary for our attacks is public information: the press analytics of URL shortening services and Twitter metadata [7]. We first evaluate tweet good reputation for Twitter users to construct time models, after which assess the advanced attack by performing experiments with virtual users following a time models. We anticipate the web site time model and also the tweet history is small because we mainly concentrate on heavy Twitter users who frequently publish tweets during each of their waking hrs. Typically, the Twitter users we examined don't publish tweets five hrs each day. Interestingly, roughly 5 % from the Twitter users publish tweets in most days

4. CONCLUSION:

We produce a Twitter user (monitoring user) who follows all of the followings from the target user to be able to access all tweets the target user may view. Through the experiments, we've proven our attacks can infer the candidates generally. In comparison, false positives are possible because some Twitter users have a similar information because the virtual users. To judge our attacks, we crawled and monitored the press analytics of URL shortening services and Twitter data. A tweet that contains a shortened URL could be read by users who aren't supporters from the user who published the tweet, via retweets or any other channels, so non-supporters may click the shortened URL. The general precision in our attack product is lower with bit.ly than by using goo.gl, because goo.gl offers four kinds of information within the click analytics. If not one other user has got the same information because the target user, our bodies can properly infer the prospective user whatever the quantity of the posting user's supporters.

REFERENCES:

[1] Jonghyuk Song, Nonmember, IEEE, Sangho Lee, Member, IEEE, and Jong Kim, Member, IEEE, "Inference Attack on Browsing History of TwitterUsers using Public Click Analytics and TwitterMetadata", IEEE Transactions on Dependable and Secure Computing, 2016.

[2] Z. Cheng, J. Caverlee, and K. Lee. You are where you tweet: A content-based approach to geo-locating twitter users. In Proc. 19th ACM International Conference on Information and Knowledge Management (CIKM), 2010.
[3] J. He, W. W. Chu, and Z. V. Liu. Inferring privacy information from social networks. In Proc.4th IEEE international conference on Intelligence and Security Informatics (ISI), 2006.
[4] S. Krishnan and F. Monrose. Dns prefetching and its privacy implications: When good things go bad. In Proc. 3rd USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET), 2010.
[5] J. Song, S. Lee, and J. Kim. I know the shortened urls you clicked on twitter: Inference attack using public click analytics and twitter metadata. In Proc. 22nd Int'l World Wide Web Conf. (WWW), 2013.
[6] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In Proc. IEEE Symp. Security and Privacy (S&P), 2010.
[7] D. boyd, S. Golder, and G. Lotan. Tweet, tweet, retweet: Conversational aspects of retweeting on twitter. In Proc. 43rd Hawaii International Conference on System Sciences (HICSS), 2010.

PROPERTY- SIMILARITY STRATEGY FOR WORKER NODE'S INTEREST

N Radhika[1]., V G Anupa[2]., B Tejaswini[3]., V.Nikitha[4]., .Priyanka[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 III Year Cse, (16RG1A05A2, 16M51A0518, 16RG1A05A5, 15RG1A05H2),

Malla Reddy College Of Engineering For Women., Maisammaguda., Medchal., Ts, India

ABSTRACT: ***We advise a singular Domain-sensitive Recommendation formula, to help make the rating conjecture by going through the user-item subgroup analysis concurrently, where a user-item subgroup is considered like a domain composed of the subset of products concentrating on the same attributes along with a subset of users who've interests during these products. The present system has some problems that might limit the performance of typical CF methods. However, it's observed this assumption isn't necessarily so tenable. This violates the matter that user's interests always focus on some specific domains, and also the users getting similar tastes on a single domain might have completely different tastes on another domain. However, typical CF methods equally treat every user and item, and can't distinguish the variation of user's interests across different domains. The suggested framework of DsRec includes three components: a matrix factorization model for that observed rating renovation, a bi-clustering model for that user-item subgroup analysis, and 2 regularization terms for connecting the above mentioned two components right into a unified formulation. Extensive experiments on Movielens-100K and 2 real-world product review datasets reveal that our method achieves the greater performance when it comes to conjecture precision qualifying criterion within the condition-of-the-art methods. To construct a concise and informative dataset for model learning, we predict to keep individuals active users and popular products in original dataset.***

Keywords: Recommender system, matrix factorization, user-item subgroup, collaborative filtering.

1. INTRODUCTION:

Numerous efforts happen to be compensated about this direction. Generally, these efforts could be split into two sorts. Nonetheless, there remain some problems that might limit the performance of typical CF methods. On a single hands, user's interests always focus on some specific domains although not all of the domains. However, the essential assumption for typical CF approaches is the fact that users rate similarly on partial products, and therefore they'll rate on the rest of the products similarly. Collaborative Filtering (CF) is an efficient and broadly adopted recommendation approach. In many of clustering CF approaches, each user or item is owned by just one cluster (domain). However, the truth is, the consumer interests and item attributes aren't always exclusive. within this paper, we advise a singular Domain-sensitive Recommendation formula aided using the user-item subgroup analysis, which integrates rating conjecture and domain recognition right into a unified framework [1]. To the very best of our understanding, our jobs are the first one to jointly think about the both tasks by only utilizing user-item interaction information. Within this paper we concentrate on the second type known as clustering CF, which only exploits the consumer-item interaction information and detects the domains by clustering methods. Collaborative Filtering (CF) is among the most effective recommendation approaches to handle mass confusion within the real life.

Literature Survey*:* Many learning designs include been employed for modeling the rating process, for example Bayesian model, regression-based model, latent semantic model, clustering model and matrix factorization model. Ungar et al. clustered users and products individually using variations of k-means and Gibbs sampling. George and Merugu acquired user and item neighborhoods via co-clustering and generated predictions in line with the average ratings from the co-clusters while using the biases from the users and products into consideration [2]. Our suggested approach differs from the above mentioned clustering CF methods. Our user-item subgroup analysis enables a person or perhaps an item to look in multiple subgroups. To be able to addresses the scalability problem, Han et al. suggested a divide-and-conquer approach. Usually, data sparsity often leads there are no common rated products for many users, who really share similar interests.

2. CLASSICAL METHOD:

Existing recommender systems happen to be indispensable nowadays, which support users with possibly different judgments and opinions within their pursuit of information, through considering the variety of preferences and also the relativity of knowledge value. Collaborative Filtering (CF) is an efficient and broadly adopted recommendation approach. Not the same as content-based recommender systems which depend around the profiles of users and products for predictions, CF approaches make predictions by only using the user-item interaction information for example transaction history or item satisfaction expressed in ratings, etc. As increasing numbers of attention is compensated on security, CF systems become more and more popular, since they don't require users to clearly condition their private information. Besides, many of these clustering CF approaches are carried out inside a two-stage consecutive process: domain recognition by clustering and rating conjecture by typical CF inside the clusters [3]. Disadvantages of existing system: However, such divide-and-conquer style brings a brand new problem, i.e., the formula cannot make the most of the observed rating data that is limited and precious. The present system has some problems that might limit the performance of typical CF methods. However, it's observed this assumption isn't necessarily so tenable. Usually, the collaborative effect among users varies across different domains.

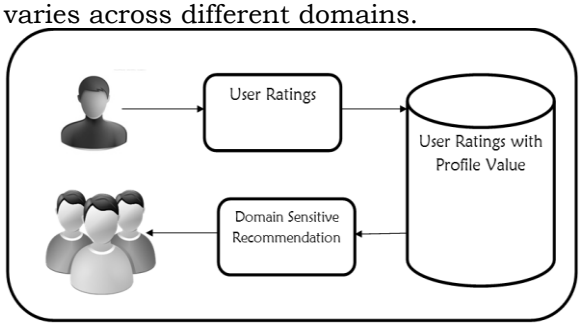


Fig.1.System architecture

3. DOMAIN-SENSITIVE METHOD:

We advise a singular Domain-sensitive Recommendation formula, to help make the rating conjecture by going through the user-item subgroup analysis concurrently, where a user-item subgroup is considered like a domain composed of the subset of products concentrating on the same attributes along with a subset of users who've interests during these products. The suggested framework of DsRec includes three components: a matrix factorization model for that observed rating renovation, a bi-clustering model for that user-item subgroup analysis, and 2 regularization terms for connecting the above mentioned two components right into a unified formulation. Extensive experiments on Movielens-100K and 2 real-world product review datasets reveal that our method achieves the greater performance when it comes to conjecture precision qualifying criterion within the condition-of-the-art methods. You will find three components within the unified framework. First, we use a matrix factorization model to best rebuild the observed rating data using the learned latent factor representations of both users and products, that individuals unobserved ratings to users and products could be predicted directly. Second, a bi-clustering model can be used to understand the arrogance distribution of every user and item owned by different domains [4]. Really, a particular domain is really a user-item subgroup, featuring it's a subset of products concentrating on the same attributes along with a subset of users interesting within the subset of products. Within the bi-clustering formulation, we think that a higher rating score rated with a user for an item encourages the consumer and also the item to become allotted to exactly the same subgroups together. Benefits of suggested system: Create a novel Domain-sensitive Recommendation formula, making rating conjecture aided using the user-item subgroup analysis. DsRec is really a unified formulation integrating a matrix factorization model for rating conjecture along with a bi-clustering model for domain recognition.

Framework Overview: The aim of DsRec would be to perform domain sensitive recommendation by jointly finding user-item subgroups and predicting domain-specific user-item correlation, where just the user-item ratings are explored. Within our framework, the domain recognition model utilizes a assumption that the high rating score rated with a user for an item encourages the consumer and also the item to become allotted to exactly the same subgroups together. The fundamental ideas behind the 3 components receive the following. With the unified model, we tightly connect the rating conjecture model and also the domain recognition model together through the two regression regularized terms [5]. First, the normal matrix factorization model is adopted to locate user-specific and item-specific latent factors to rebuild the observable user-item ratings, so we can make use of the learned factors to calculate the rating associated with a user

item pair. Second, a bi-clustering model is formulated to take advantage of the duality between users and products to cluster them into subgroups. Third, the regression regularization tries to discover the mappings in the latent factor representations of users for their confidence distribution. More to the point, the resulting co-clustered subgroups may reveal valuable insights in the item attributes. The concept behind the regression regularization would be that the latent factor representations of users are needed to mirror the preferences of users across different domains. Within this paper, we create a novel Domain-sensitive Recommendation formula, making rating conjecture aided using the user-item subgroup analysis [6]. DsRec is really a unified formulation integrating a matrix factorization model for rating conjecture along with a bi-clustering model for domain recognition. To construct a concise and informative dataset for model learning, we predict to keep individuals active users and popular products in original dataset. We first remove sparsity by filling the missing data within the user-item rating matrix using the average rating from the corresponding item. Within the comparison, the very first three methods are traditional and popular collaborative recommendation techniques without thinking about the domain influence, and yet another four methods are clustering based collaborative recommendation techniques. Our method DsRec consistently outperforms other approaches out of all settings on these 3 datasets. This verifies the potency of our method. Not the same as other matrix factorization methods, there's a substantial character for WNMF that is more sensitive using the change from the latent factor dimension [7]. The parameter controls just how much impact is functioned between your rating predication model and also the domain recognition model. only importing the regression regularization terms, the rating conjecture model and also the domain recognition model could be truly linked to carry out the domain-sensitive recommendation. Later on, we'll make an effort to explore both user-item interaction information and a few exterior information concurrently for domain recognition.

4. CONCLUSION:

Our method DsRec consistently outperforms other approaches out of all settings on these 3 datasets. This verifies the potency of our method. Not the same as other matrix factorization methods, there's a substantial character for WNMF that is more sensitive using the change from the latent factor dimension. Systematic experiments conducted on three real-world datasets demonstrate the potency of our methods. It's important to note our technique is totally in line with the user-item rating matrix. Motivated through the observation, within this paper, we advise a singular Domain-sensitive Recommendation formula, to help make the rating conjecture by going through the user-item subgroup analysis concurrently, where a user-item subgroup is considered like a domain composed of the subset of products concentrating on the same attributes along with a subset of users who've interests during these products. Furthermore, information between both of these components is exchanged through two regression regularization products, so the domain information guides the search for the latent space. Within our framework, the domain recognition model utilizes a assumption that the high rating score rated with a user for an item encourages the consumer and also the item to become allotted to exactly the same subgroups together.

REFERENCES:

[1] Jing Liu, Member, IEEE, Yu Jiang, Zechao Li, Member, IEEE, Xi Zhang,and Hanqing Lu, Senior Member, IEEE, “Domain-Sensitive Recommendationwith User-Item Subgroup Analysis”, ieee transactions on knowledge and data engineering, vol. 28, no. 4, april 2016.

[2] S. Zhang, W. Wang, J. Ford, and F. Makedon, “Learning from incomplete ratings using non-negative matrix factorization,” in Proc. 6th SIAM Int. Conf. Data Mining, 2006, pp. 549–553.

[3] A. Bellogin and J. Parapar, “Using graph partitioning techniques for neighbour selection in user-based collaborative filtering,” in Proc. 6th ACM Conf. Recommender Syst., 2012, pp. 213–216.

[4] J. L. Herlocker, J. A. Konstan, A. Borchers, and J. Riedl, “An algorithmic framework for performing collaborative filtering,” in Proc. 22nd Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 1999, pp. 230–237.

[5] Y. Zhang, B. Cao, and D.-Y. Yeung, “Multi-domain collaborative filtering,” in Proc. 26th Conf. Annu. Conf. Uncertainty Artif. Intell., 2010, pp. 725–732.

[6] C. Chen, X. Zheng, Y. wang, F. Hong, and Z. Lin, “Context-aware collaborative topic regression with social matrix factorization for recommender systems,” in Proc Conf. Artif. Intell., 2014, pp. 9–15

PROVIDING HUGE EMBEDDING POWER TO RECONSTRUCT ORIGINAL VISUAL

P. Lavanya[1]., U Tejasree[2]., P.Susmitha[3]., Seelam Sanjana[4]., P.Bindu Manasa[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ 534nagendra@gmail.com)

2, 3, 4, 5 B.Tech III Year CSE, (16RG1A0598, 16RG1A0574, 16RG1A0592, 16RG1A0579),

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

ABSTRACT: ***A lot of the existing RIDH algorithms are made within the plaintext domain, namely, the content bits take root in to the original, united nations-encrypted images. To safeguard the security and privacy, all images is going to be encrypted prior to being given to a united nations-reliable 3rd party for more processing. For security reasons, any base station doesn't have privilege of being able to access the key file encryption key K pre-negotiated between your satellite and also the data center. This means the message embedding operations need to be conducted entirely within the encrypted domain. the ciphertext is generated by bitwise XORing the plaintext using the key stream. Otherwise specified, the broadly used stream cipher AES within the CTR mode is assumed. It's emphasized that the potential of eliminating the information hiding secret is not unique to the suggested method, but instead perhaps relevant for those non-separable RIDH schemes over encrypted domain. Within our suggested RIDH plan, the information hiding key continues to be eliminated, and therefore, both of these attack models aren't relevant. We have performed extensive experiments to validate the highest embedding performance in our suggested RIDH method over encrypted domain. In contrast to the condition-of-the-arts, the suggested approach provides greater embedding capacity, and has the capacity to perfectly rebuild the initial image along with the embedded message. In contrast to the condition-of-the-arts, the suggested approach provides greater embedding capacity, and has the capacity to achieve perfect renovation from the original image along with the embedded message bits.***

Keywords: Satellite data center, reversible image data hiding (RIDH), signal processing over encrypted domain, feature extraction.

1. INTRODUCTION:

An all natural question arising now's whether we are able to design an encrypted-domain RIDH plan, which doesn't need a secret data hiding key, while still making certain that just the party using the secret file encryption key K can disclose the embedded message. Within this paper, we design a safe and secure reversible image data hiding (RIDH) plan operated within the encrypted domain [1]. We recommend an open key modulation mechanism, which enables us to embed the information via simple XOR operations, with no need of being able to access the key file encryption key. Within this work, we advise an encrypted-domain RIDH plan by particularly using the above-pointed out design preferences into account. Within this work, we don't think about the situation of embedding multiple watermarks for just one single block, and therefore each block is processed once for the most part. the Known Original Attack (KOA), where the attacker can access several pairs of formerly watermarked images and also the corresponding cover image. Certainly, the present cover image isn't recognized to the attacker. Under theWOA, the only real attack type highly relevant to our plan, the attacker tries to extract the embedded message and/or recover the initial image in the watermarked and encrypted image. Certainly, the information hiding key must be shared and managed between your date hider and also the recipient. In contrast to the initial, united nations-encrypted block, the pixels within the encrypted block generally have an infinitely more uniform distribution. This motivates us introducing the neighborhood entropy in to the feature vector to capture such distinctive characteristics. As pointed out earlier, the important thing management functions, e.g., the important thing generation, activation, de-activation, suspension, expiration, destruction, archival, and revocation, take time and effort to become reliably implemented within such distributed infrastructure [2].

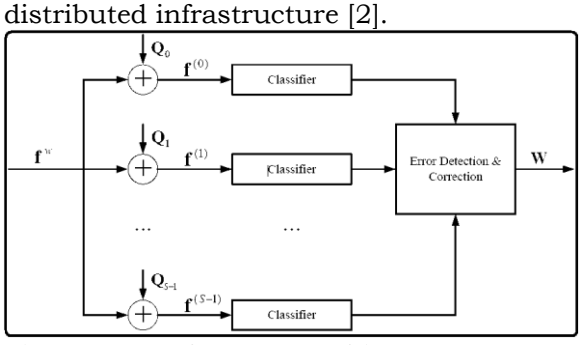


Fig.1.Proposed system architecture

2. METHODOLOGY:

The formula produced by MacDonald may be used to this finish. Observe that all of the public keys are made in to the data hider and

also the recipient once the whole system is to establish, and therefore, there is no need to deliver them throughout the data embedding stage. The information embedding is achieved via a public key modulation mechanism, by which accessibility secret file encryption secret is unnecessary [3]. The most recent difference expansion (DE)-based schemes and also the improved conjecture error expansion (PEE)-based strategies were proven so that you can provide the condition-of-the-art capacity distortion performance. The content indistinguishability signifies that the attacker can perform no much better than simple random guessing if he only observes the ciphertext. This rentals are considered like a fundamental requirement of any secure file encryption plan. Zhang et. al. extended the lossless compression based RIDH method of the encrypted domain, namely, listlessly compress 1 / 2 of the fourth LSBs from the encrypted image via LDPC code to produce space for data hiding. Therefore, the attacker trying to extract the embedded message bits from [[f]]w will be able to don' much better than random guessing [4]. This proves the safety in our suggested encrypted-domain RIDH strategy against WOA attack. In the decoder side, a effective two-class SVM classifier is made to distinguish encrypted and non-encrypted image patches, allowing us to jointly decode the embedded message and also the original image signal. Both strategies could be readily implemented used with minimal affect towards the actual embedding rate. With regard to simpler presentation, we exclude the discussion of embedding A within the follow up. we highlight the blocks by which extraction errors exist in the 2 problematic images when n = 8. To tackle this concern, a mistake-correcting code (ECC) for example Hamming code may be used to further correct individuals unsolvable errors, at the expense of considerably reduced embedding rate [5]. It may be observed the incorrectly decoded blocks are untypically homogenous in textural characteristics for their context, which is the problem in discretion through the suggested error correction mechanism. When classification errors are detected for many blocks, we want a mechanism to fix them. Although the classifier is carefully designed, it's still hard to distinguish individual's highly textured original blocks in the encrypted ones, particularly when the block dimensions are small. Before presenting the information extraction and image understanding methods, let's first investigate features you can use to discriminate encrypted and non-encrypted image blocks. The classifier designed based on these functions is going to be proven to become essential in the suggested joint data extraction and image understanding approach. The suggested technique embeds message via a public key modulation mechanism, and performs data extraction by exploiting the record distinguish ability of encrypted and non-encrypted image blocks [6]. Because the decoding from the message bits and also the original image is tied together, our suggested technique is one of the group of non-separable RIDH solutions. Our method can embed 21675 message bits for every 512×512 image once the block dimensions are 6×6, while making certain 100% precision of information extraction. Because the block size decreases further, few extraction errors appear.

3. ENCRYPTED IMAGES:

Our suggested RIDH plan over encrypted domain can also be extended to deal with compressed and encrypted images, namely, embed watermark in to the compressed and encrypted bit stream. Upon understanding the characteristics and behavior from the decoding error, the job of designing and applying an ECC turns into a trivial issue. In contrast to the condition-of-the-arts, the suggested approach provides greater embedding capacity, and has the capacity to perfectly rebuild the initial image along with the embedded message. In contrast to the condition-of-the-arts, the suggested approach provides greater embedding capacity, and has the capacity to achieve perfect renovation from the original image along with the embedded message bits. In contrast to the initial, united nations-encrypted block, the pixels within the encrypted block generally have an infinitely more uniform distribution.

4. CONCLUSION:

This motivates us introducing the neighborhood entropy in to the feature vector to capture such distinctive characteristics. The off-line trained SVM classifier will be employed to discriminate the encrypted and non-encrypted image patches while data extraction and image understanding. Realizing the joint understanding and knowledge extraction of various blocks are largely independent, except the mistake correction stage where image self-similarity is exploited, significant time saving could be retained using a parallel computing platform.

REFERENCES:

[1] C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao, "An in painting-assisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109-1118, 2013.

[2] M. Barni, F. P., R. Lazzeretti, A.-R. Sadeghi, and T. Schneider," Privacy preserving ecg classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 2, pp. 452-468, 2011.

[3] F. Cayre, C. Fontaine, and T. Furon,"Watermarking security: theory and practice," IEEE Trans. Sig. Proc., vol. 53, no. 10, pp. 3976-3987, 2005.

[4] M. U. Celik, G. Sharma, and A. M. Tekalp," Lossless watermarking for image authentication: a new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042-1049, 2006.

[5] T. Bianchi, A. Piva, and M. Barni,"On the implementation of the discrete fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Secur., vol. 4, no. 1, pp. 86-97, 2009.

[6] Y. Hu, H. K. Lee, and J. Li,"De-based reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250-260, 2009.

SCALING COMPLEXITY AND INEFFICIENT OPERATIONS IN OPEN NETS

Kurla Kranthi[1]., B.Sakshi [2]., R.Likhitha[3]., R Harshith[4] ., P.Manisha Yadav[5]

1 Assistant Professor, Department of CSE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ saiduluvcse@vjit.ac.in)

2, 3, 4,5 B.Tech III Year CSE, (16RG1A0587, 16RG1A0586, 16RG1A0582, 16RG1A0578),

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

ABSTRACT: ***A brand new system architecture to handle fine-grained RDF partitions in large-scale. Novel data placement strategies to co-locate semantically related bits of data. Within this paper, we describe RpCl, a competent and scalable distributed RDF data management system for that cloud. Unlike previous approaches, RpCl runs a physiological analysis of both instance and schema information just before partitioning the information. The machine keeps a sliding-window w tracking the current good reputation for the workload, in addition to related statistics about the amount of joins that needed to be performed and also the incriminating edges. The machine combines join ahead pruning via RDF graph summarization having a locality- based, horizontal partitioning from the triples right into a grid like, distributed index structure. The Important Thing Index is a vital index in RpCl it utilizes a lexicographical tree to parse each incoming URI or literal and assign it a distinctive number key value. Sharding such data using classical techniques or partitioning the graph using traditional min-cut algorithms results in very inefficient distributed operations and also to a higher quantity of joins. Many RDF systems depend on hash-partitioning as well as on distributed selections, projections, and joins. Grid-Vine system was among the first systems to do this poor large-scale decentralized RDF management. Within this paper, we describe the architecture of RpCl, its primary data structures, along with the new algorithms we use to partition and distribute data. We produce an extensive look at RpCl showing our product is frequently two orders of magnitude quicker than condition-of-the-art systems on standard workloads.***

Keywords: Key Index, RDF, triple stores, cloud computing, Big data.

1. INTRODUCTION:

We advise RpCl, a competent, distributed and scalable RDF information systems system for distributed and cloud environments. Typically, relational information systems is scaled out by partitioning the relations and rewriting the query intends to reorder operations and employ distributed versions from the operators enabling intra-operator parallelism. a brand new system architecture to handle fine-grained RDF partitions in large-scale. Despite recent advances in distributed RDF data management, processing large-levels of RDF data within the cloud continues to be very challenging [1]. Regardless of its apparently simple data model, RDF really encodes wealthy and sophisticated graphs mixing both instance and schema-level data. The machine seemed to be extended in TripleProv to aid storing, tracking, and querying provenance in RDF query processing. Embarrassingly parallel problems could be relatively easily scaled in the cloud by launching new processes on new commodity machines.

Previous Study: GridVine system utilizes a triple-table storage approach and hash-partitioning to distribute RDF data over decentralized P2P systems. Wilkinson et al. propose using two kinds of property tables: one that contains clusters of values for qualities which are frequently co-utilized together, and something exploiting the kind property of subjects to cluster similar teams of subjects together within the same table. An identical approach is suggested by Harris et al. where they use a simple storage model storing quads of. Information is partitioned as non-overlapping teams of records among segments of equal subjects Methods for storing RDF data could be broadly categorized in three subcategories: triple-table approaches, property table approaches, and graph-based approaches. We lately labored with an empirical evaluation to look for the extent that such no SQL systems may be used to manage RDF data within the cloud Zeng et al. build on the top of Trinity and implement an in-memory RDF engine storing data inside a graph form. Our bodies is made on three primary structures: RDF molecule clusters, template lists as well as an efficient key index indexing URIs and literals in line with the clusters they fit in with [2].

2. CLASSICAL SCHEME:

While a lot more recent than relational data management, RDF data management has lent many relational techniques Methods for storing RDF data could be broadly categorized in three subcategories: triple-table approaches, property-table approaches, and graph-based approaches. Hexastore suggests to index RDF data using six possible indices, one for every permutation from the group of posts within the

triple table. RDF-3X and YARS consume a similar approach. BitMat keeps a three-dimensional bit-cube where each cell represents a distinctive triple and also the cell value denotes presence or lack of the triple. Various techniques offer speed-up RDF query processing by thinking about structures clustering RDF data according to their qualities. Disadvantages of existing system: Existing system generates much inter-process traffic, considering that related triples finish up being scattered on all machines. RDF really encodes wealthy and sophisticated graphs mixing both instance and schema-level data. Sharding such data using classical techniques or partitioning the graph using traditional min-cut algorithms results in very inefficient distributed operations and also to a higher quantity of joins. Existing system aren't efficient and never scalable system for managing RDF data within the cloud. Existing system are slower while handling the conventional workloads.

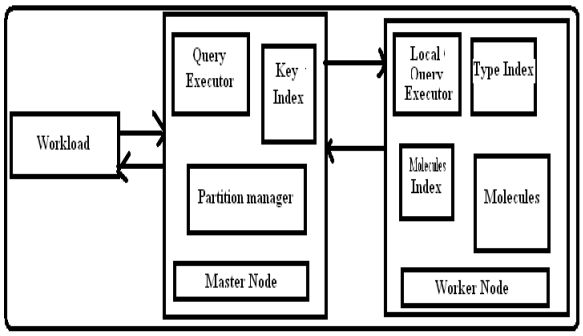


Fig.1.System Framework

3. ENHANCED DESIGN:

In the following paragraphs, we advise RpCl, a competent, distributed and scalable RDF information systems system for distributed and cloud environments. Unlike many distributed systems, RpCl utilizes a resolutely non-relational storage format, where semantically related data patterns are found both in the instance-level and also the schema-level data and obtain co-located to reduce inter node operations [3]. The primary contributions want to know , are: A brand new hybrid storage model that wisely partitions an RDF graph and physically co-locates related instance data A brand new system architecture to handle fine-grained RDF partitions in large-scale Novel data placement strategies to co-locate semantically related bits of data New data loading and query execution strategies benefiting from our system's data partitions and indices A comprehensive experimental evaluation showing our product is frequently two orders of magnitude quicker than condition-of-the-art systems on standard workloads benefits of suggested system: RpCl is an excellent and scalable system for managing RDF data within the cloud. RpCl is especially suitable for clusters of commodity machines and cloud environments where network latencies could be high, because it systematically attempts to avoid all complex and distributed operations for query execution.

Clustering Model: Molecule clusters are utilized in 2 ways within our system: to logically group teams of related URIs and literals within the hash table, and also to physically co-locate information associated with confirmed object on disk as well as in primary memory to lessen disk and CPU cache latencies. Resistant to the property-table and column-oriented approaches, our bodies according to templates and molecules is much more elastic, meaning that every template could be modified dynamically. Queries that can't be performed without inter-nodes communication are decomposed into sub-queries. The machine combines join ahead pruning via RDF graph summarization having a locality- based, horizontal partitioning from the triples right into a grid like, distributed index structure [4]. The Important Thing Index is a vital index in RpCl it utilizes a lexicographical tree to parse each incoming URI or literal and assign it a distinctive number key value. The authors of the paper develop an easy hash partitioning and hop-based triple replication. We make use of a tailored lexicographic tree to parse URIs and literals and assign them a distinctive number ID. The clusters contain all triples departing in the root node when traversing the graph, until another demonstration of a root node is entered. In situation a brand new template is detected, then your template manager updates its in-memory triple template schema and inserts new template IDs to mirror the brand new pattern it discovered. Finally, the molecules are defined to be able to materialize frequent joins, for instance between a business and it is corresponding values, or between two semantically related entities which are frequently co-utilized [5]. RpCl uses physiological RDF partitioning and molecule patterns to efficiently co-locate RDF data in distributed settings. Much like web site lists, the molecule clusters are serialized in an exceedingly compact form, both on disk as well as in primary-memory Auxiliary Indexes: While creating molecule templates and molecules

identifiers, our bodies also take Ares of two additional data gathering and analysis tasks.

System Framework: Our bodies design follows the architecture of numerous modern cloud-based distributed systems, where one (Master) node accounts for getting together with the clients and orchestrating the operations done by another nodes. The Actual may also be duplicated to scale the key index for very large datasets, in order to replicate the dataset around the Workers using different partitioning schemes the employees tend to be simpler compared to Master node and therefore are built on three primary data structures: i) a kind index, ii) a number of RDF molecules, and iii) a molecule index.

Data Partitioning and Allocation: The easiest technique is to by hand define numerous template types becoming root nodes for that molecules, after which to co-locate all further nodes which are directly or not directly attached to the roots, as much as given scope k [6]. By using this technique, the administrator essentially specifies, according to resource types, the precise path following which molecules ought to be physically extended. When the physiological partitions are defined, RpCl still faces the option of how you can distribute the concrete partitions over the physical nodes. The benefit of this process is it starts with easy little data structures after which instantly adapts towards the dynamic workload by growing.

Frequent Practices: We essentially trade relatively complex instance data examination and sophisticated local co-place for faster query execution. We think that the information to become loaded will come in a shared space around the cloud. RpCl is an excellent and scalable system for managing RDF data within the cloud. From your perspective, it strikes an ideal balance between intra-operator parallelism and knowledge collocation by thinking about recurring, fine-grained physiological RDF partitions and distributed data allocation schemes, leading however to potentially bigger data and also to more complicated inserts and updates. they may be processed directly within our system by updating the important thing index, the related cluster, and also the template lists if required. Query processing in RpCl is quite different from previous methods to execute queries on RDF data, due to the three peculiar data structures within our system: Because the RDF nodes are logically grouped by molecules within the key index, it is normally sufficient to see the related listing of molecules within the molecules index [7]. Generally, the important thing index is invoked to obtain the corresponding molecule For the easiest and also the most generic one, we divide the query into three fundamental graph patterns so we prepare intermediate results on every node the 2nd method, we similarly divide the query into three fundamental graph patterns so we prepare, on every node, intermediate recent results for the very first constraint The 3rd and many efficient strategy is always to boost the scope from the considered molecules. We've implemented a prototype of RpCl following a architecture and methods described above. We observe that in the present prototype we didn't implement dynamic updates. We prevented the artifact of connecting towards the server, initializing the DB from files and printing recent results for all systems The slowest may be the path query that involves several joins. For those individuals queries RpCl performs perfectly.

4. CONCLUSION:

Around the worker nodes, building the molecule is definitely an n-pass formula in RpCl, since we have to construct the RDF molecules within the clusters. To deal with them efficiently, we adopt a lazy rewrite strategy, much like much modern read-enhanced system. In-place updates are punctual updates on literal values finally, we're presently testing and increasing our bodies with several partners to be able to manage very-massive, distributed RDF datasets poor bioinformatics applications. RpCl is especially suitable for clusters of commodity machines and cloud environments where network latencies could be high, because it systematically attempts to avoid all complex and distributed operations for query execution. We intend to continue developing RpCl in a number of directions: First, we intend to start adding some further compression mechanisms. We intend to focus on a computerized templates discovery according to frequent patterns and untied elements. Also, we intend to focus on integrating an inference engine into RpCl to aid a bigger group of semantic constraints and queries natively. Our experimental evaluation demonstrated it very favorably comes even close to condition-of-the-art systems such environments.

REFERENCES:

[1] Marcin Wylot and Philippe Cudr_e-Mauroux, "RpCl: Efficient and Scalable Managementof RDF Data in the Cloud", ieee transactions on knowledge and data engineering, vol. 28, no. 3, march 2016.

[2] Y. Guo, Z. Pan, and J. Heflin, "An evaluation of knowledge base systems for large OWL datasets," in Proc. Int. Semantic Web Conf., 2004, pp. 274–288.

[3] M. Wylot, P. Cudre-Mauroux, and P. Groth, "TripleProv: Efficient processing of lineage queries in a native RDF store," in Proc. 23rd Int. Conf. World Wide Web, 2014, pp. 455–466.

[4] A. Kiryakov, D. Ognyanov, and D. Manov, "OWLIM–a pragmatic semantic repository for OWL," in Proc. Int. Workshops Web Inf. Syst. Eng. Workshops, 2005, pp. 182–192.

[5] M. Br€ocheler, A. Pugliese, and V. Subrahmanian, "Dogma: A diskoriented graph matching algorithm for RDF databases," in Proc. 8th Int. Semantic Web Conf., 2009, pp. 97–113.

[6] K. Rohloff and R. E. Schantz, "Clause-iteration with MapReduce to scalably query datagraphs in the shard graph-store," in Proc. 4th Int. Workshop Data-Intensive Distrib. Comput., 2011, pp. 35–44.

STEADY CONTACT POLICY WITH DECREASED SIZE OF SECRET CODE

V Sireesha[1]., P Akanksha[2]., T Snehitha[3]., T Susmitha[4]., P Keerthi[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 III Year CSE, (16RG1A0572, 16RG1A0595, 16RG1A0596, 16RG1A0573),

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

ABSTRACT: Inside a Clubpenguin-ABE, the user's attributes employed for key generation must fulfill the access policy employed for file encryption to be able to decrypt the ciphertext, during a KP-ABE, the consumer are only able to decrypt ciphertexts whose attributes fulfill the policy baked into the important thing. Our new technique results in a new Clubpenguin-ABE plan with constant ciphertext size, which, however, cannot hide the access policy employed for file encryption. The present ABE schemes according to AND-Gate with wildcard cannot accomplish this property. ABE can well safeguard the secrecy from the encrypted data against unauthorized access; it doesn't safeguard the privacy from the receivers/decryptions automatically. Our new technique results in a new Clubpenguin-ABE plan with constant ciphertext size. Within the full security model, the foe can pick the task policy within the Challenge phase, making the model more powerful. We demonstrated our second construction is safe underneath the Decisional Bilinear Diffie-Hellman and also the Decision Straight line assumptions. One disadvantage in our second construction is the fact that its ciphertext size is not constant, and then showing this construction in fully secure. The machine used within the first construction to bridge ABE according to AND-Gate with wildcard with Inner Product File encryption (IPE). Particularly, we place the indices of the entire positive, negative and wildcard attributes defined within an access structure into three sets, and using the manner of Viète's formulas.

Keywords: Attribute based encryption, hidden policy, inner product encryption, Viète's formula.

1. INTRODUCTION:

Within this work, we explore new approaches for the making of Clubpenguin-ABE schemes in line with the AND-gate with wildcard access structure. A user's attributes will be based on a string of good and bad symbols w.r.t. each attribute within the world. We advise two new ciphertext policies attribute based file encryption (Clubpenguin-ABE) schemes in which the access policy is determined by AND-gate with wildcard. There are various methods to define an access structure/insurance policy for ABE. Therefore, it's also necessary for hide the access policy such applications [1] [2]. We use p to indicate the pairing operation, n the amount of attributes within an access structure or attribute list, m the amount of all possible values for every attribute, and w the amount of wildcard within an access structure. The primary contribution of the paper would be to propose a brand new Clubpenguin-ABE plan using the property of hidden access policy by extending the process we utilized in the making of our first plan [3].

2. TRADITIONAL SCHEME:

Within the first plan, we present a brand new technique that utilizes just one group element to represent a characteristic, as the existing ABE schemes of the identical type want to use three different group elements to represent a characteristic for those three possible values. The fuzzy IBE provided by Sahai and Waters, which may be treated because the first KP-ABE used a particular threshold access policy. Later, the Straight-line Secret Discussing Plan (LSSS) realizable (or monotone) access structure continues to be adopted by many people subsequent ABE schemes [4]. Cheung and Newport suggested a different way to define access structure using AND-Gate with wildcard. Cheung and Newport demonstrated that applying this simple access structure that is sufficient for a lot of applications, Clubpenguin-ABE schemes could be built according to standard complexity assumptions. Subsequently, several ABE schemes were suggested after this specific access structure. Disadvantages of existing system: The present ABE schemes according to AND-Gate with wildcard cannot accomplish this property. ABE can well safeguard the secrecy from the encrypted data against unauthorized access; it doesn't safeguard the privacy from the receivers/decryptions automatically. That's, because of the ciphertext, an unauthorized user can always have the ability to obtain some good info from the data recipients. Although a safe and secure ABE can well safeguard the secrecy from the encrypted data against unauthorized access, it

doesn't safeguard the privacy from the receivers/decryptions automatically. That's, because of the ciphertext, an unauthorized user can always have the ability to obtain some good info from the data recipients. For instance, any adverse health organization really wants to send a note to any or all the patients that carry certain illnesses. Then your attribute world contains all of the illnesses, as well as an access policy may have the format "** . . ." where "" ("-") signifies positive (negative) for the disease. If your Clubpenguin-ABE cannot hide the access policy, then in the fact whether an individual can decrypt the content or otherwise, people can directly learn some sensitive information from the user. Therefore, it's also necessary for hide the access policy such applications. However, the majority of the existing ABE schemes according to AND-Gate with wildcard cannot accomplish this property [5].

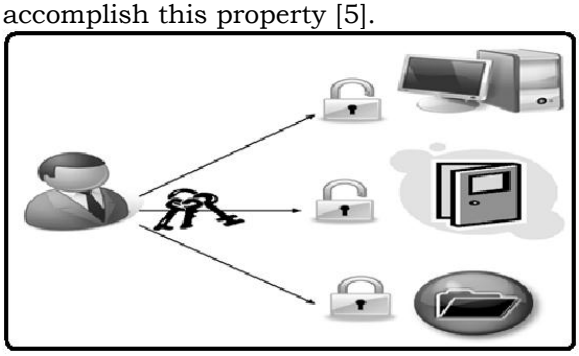


Fig.1.Proposed framework

3. ENHANCED PROPOSAL:

Within this work, we explore new approaches for the making of Clubpenguin-ABE schemes in line with the AND-gate with wildcard access structure. The present schemes of the type want to use three different elements to represent the 3 possible values - positive, negative, and wildcard - of the attribute within the access structure. Within this paper, we advise a brand new construction which utilizes just one element to represent one attribute. The primary idea behind our construction is by using the "positions" of various symbols to do the matching between your access policy and user attributes. Particularly, we place the indices of all of the positive, negative and wildcard attributes defined within an access structure into three sets, and using the manner of Viète's formulas, we permit the decrypt or to get rid of all of the wildcard positions, and carry out the understanding properly if and just when the remaining user attributes match individuals defined within the access structure. We further read the problem of hiding the access insurance policy for Clubpenguin-ABE according to AND-Gate with wildcard. Because the primary contribution of the work, we extend the process we've utilized in the very first construction to bridge ABE according to AND-Gate with wildcard with Inner Product File encryption (IPE). We demonstrated our second construction is safe underneath the Decisional Bilinear Diffie-Hellman and also the Decision Straight line assumptions [6]. One disadvantage in our second construction is the fact that its ciphertext size is not constant, and then showing this construction in fully secure. We leave the answer with this problem as our future work. Particularly, we present a method to convert an access policy that contains positive, negative, and wildcard symbols right into a vector _X which is often used for file encryption, and also the user's attributes that contains good and bad symbols into another vector _ Y which is often used in key generation, after which use the manner of IPE to complete the file encryption. Benefits of suggested system: Our new technique results in a new Clubpenguin-ABE plan with constant ciphertext size. The machine used within the first construction to bridge ABE according to AND-Gate with wildcard with Inner Product File encryption (IPE). Our first plan achieves constant ciphertext size. Secure underneath the Decisional Bilinear Diffie-Hellman and also the Decision Straight line assumptions.

Clubpenguin-ABE: Within this paper, we presented two new constructions of Ciphertext Policy Attribute Based File encryption for that AND-Gate with wildcard access policy. Our first plan achieves constant ciphertext size, but cannot hide the access policy. We prove our second plan is safe underneath the standard decisional straight line and decisional bilinear Diffie-Hellman assumptions. One method to attain the attribute hiding property is to use the interior Product File encryption technique in the making of Clubpenguin-ABE [7]. Since our plan really uses the vector akin to an access policy to complete the file encryption. To be able to prove our plan is policy hiding, we only have to prove the foe cannot tell which vector. Particularly, we show a method to bridge ABE according to AND-gate with wildcard with inner product file encryption after which make use of the latter to offer the objective of hidden access policy.

4. CONCLUSION:

Inside a Clubpenguin-ABE, the user's attributes employed for key generation must fulfill the access policy employed for file encryption to be able to decrypt the ciphertext, during a KP-ABE, the consumer are only able to decrypt ciphertexts whose attributes fulfill the policy baked into the important thing. We are able to observe that access control is definitely a natural feature of ABE, by with a couple significant access structures, we are able to effectively achieve fine-grained access control. However, our second plan may even hide the access policy from the legitimate decryptions. Within this paper, we advise a brand new construction which utilizes just one element to represent one attribute. The main idea behind our construction is by using the "positions" of various symbols to do the matching between your access policy and user attributes.

REFERENCES:

[1] Tran Viet Xuan Phuong, Guomin Yang, Member, IEEE, and Willy Susilo, Senior Member, IEEE, "Hidden Ciphertext Policy Attribute-BasedEncryption Under Standard Assumptions", ieee transactions on information forensics and security, vol. 11, no. 1, january 2016.

[2] S. Sedghi, P. van Liesdonk, S. Nikova, P. Hartel, and W. Jonker, "Searching keywords with wildcards on encrypted data," in Security and Cryptography for Networks (Lecture Notes in Computer Science), vol. 6280. Berlin, Germany: Springer-Verlag, 2010, pp. 138–153.

[3] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in Proc. 5th Int. Conf. Provable Secur. (ProvSec), 2011, pp. 84–101.

[4] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in Proc. 17th Austral. Conf. Inf. Secur. Privacy, 2012, pp. 336–349.

[5] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. Theory Appl. Cryptogr. Techn. 27th Annu. Int. Conf. Adv. Cryptol. (EUROCRYPT), 2008, pp. 146–162.

[6] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 90–108.

[7] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Computationally efficient ciphertext-policy attribute-based encryption with constantsize ciphertexts," in Provable Security. New York, NY, USA: Springer-Verlag, 2014, pp. 259–273.

USER GROUP'S UPDATABLE PRIVATE KEY SHARING SCHEME FOR OPEN SYSTEMS

P Swetha Nagasri[1]., Neela Teja[2]., T Susmitha[3]., T Archana[4]., M Supriya[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 III Year CSE, (16RG1A0566, 16RG1A0594, 16RG1A0597, 16RG1A0562),

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

ABSTRACT: ***Within the existing plan, whenever a user leaves from the user group, the audience manager only revokes his group secret key which means the user's private key connected with attributes continues to be valid. Our plan is appropriate for resource restricted devices. If a person within the group intentionally exposes the audience secret answer to the revoked user, he is able to perform understanding operations through his private key. To explain this attack, a concrete instance is offered. We prove the safety in our plan underneath the divisible computation Diffie-Hellman (DCDH) assumption. Regrettably, ABE plan requires high computation overhead during performing file encryption and understanding operations. This defect gets to be more severe for lightweight devices because of their restricted computing sources. Within this system, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. Caused by our experiment shows computation cost for local devices is comparatively low and could be constant. We try to model collusion attack done by revoked users cooperating with existing users. In addition, we construct a competent user revocation Club penguin-ABE plan through increasing the existing plan and prove our plan is CPA secure underneath the selective model.***

Keywords: outsourced encryption, cloud computing, collusion attack, attribute-based encryption, user revocation.

1. INTRODUCTION:

The problem of user revocation could be solved efficiently by presenting the idea of user group. When any user leaves, the audience manager will update users' private keys aside from individuals who've been revoked. Furthermore, Club penguin-ABE plan has heavy computation cost, because it grows linearly using the complexity for that access structure. To lessen the computation cost, we delegate high computation load to cloud providers without dripping file content and secret keys [1]. Particularly, our plan can with stand collusion attack done by revoked users cooperating with existing users. To lessen the computation cost for resource-restricted devices, some cryptographic operations rich in computational load were outsourced to cloud providers. Combined proxy re-file encryption with lazy re-file encryption technique, Eco-friendly et al. provided a competent Club penguin-ABE plan with outsourcing understanding. Within their plan, user's private secret is blinded through utilizing a random number. Both private key and also the random number are stored secret through the user. The consumer shares his blinded private answer to a proxy to do outsourced understanding operation [2]. To be able to safeguard privacy from the user, Han et al. presented a decentralized KP-ABE plan with privacy-preserving. Similarly, Qian et al. provided a decentralized Club penguin-ABE with fully hidden access structure. In the following paragraphs, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. We try to model collusion attack done by revoked users cooperating with existing users. Can't. When user1is revoked in the group, he can't decrypt alone because he doesn't possess the updated group secret key. We construct a competent user revocation Club penguin-ABE plan through increasing the plan and prove our plan is CPA secure underneath the selective model. To resolve above security issue, we embed certificates into each user's private key. The consumer shares his blinded private answer to a proxy to do outsourced understanding operation. Within this paper, we make use of the similar techniques regarding ex-tend our plan with outsourcing ability.

2. TRADITIONAL MODEL:

Boldyreva et al. presented an IBE plan with efficient revocation, also is appropriate for KP-ABE. Nonetheless, it's not obvious whether their plan is appropriate for Club penguin-ABE. Yu et al. provided a characteristic based data discussing plan with attribute revocation ability. This plan was demonstrated to become secure against selected plaintext attacks (CPA) according to DBDH assumption. However, the size of cipher text and user's private key are proportional to the amount of attributes within the attribute world. Yu et al. developed a KP-ABE plan with fine-grained data access control [3]. This plan mandates that the main node

within the access tree is definitely an AND gate and something child is really a leaf node that is connected using the dummy attribute. Think that the information is encrypted underneath the policy "professor AND cryptography" and also the group public key. Suppose there are two users: user1and user2 whose private keys are connected using the attribute sets and correspondingly. If are both within the group and contain the group secret key, then user1can decrypt the information but user2can't. When user1is revoked in the group, he can't decrypt alone because he doesn't possess the updated group secret key. However, the features of user1are not revoked and user2 has got the updated group secret key. So, user1can collude with user2 to do the understanding operation. In addition, security model and proof weren't provided within their plan. Disadvantages of existing system: It's costly in communication and computation cost for users. There's a significant limitation to single-authority ABE as with IBE. Namely, each user authenticates him towards the authority, proves he includes a certain attribute set, after which receives secret key connected with every of individuals attributes. Thus, the authority should be reliable to watch all of the attributes. It's not reasonable used and cumbersome for authority [4].

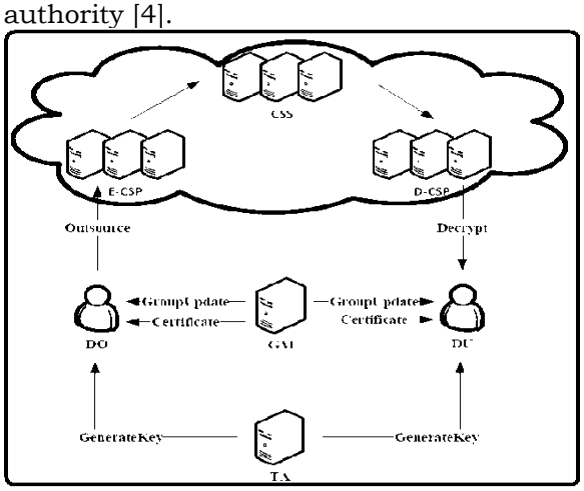


Fig.1.System Framework

3. COLLUSION FREE SCHEME:

Within this system, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. We try to model collusion attack done by revoked users cooperating with existing users. In addition, we construct a competent user revocation Club penguin-ABE plan through increasing the existing plan and prove our plan is CPA secure underneath the selective model. To resolve existing security issue, we embed certificates into each user's private key. In this manner, each user's group secret key differs from others and bound along with his private key connected with attributes [5]. To lessen users' computation burdens, we introduce two cloud providers named file encryption-cloud company (E-CSP) and understanding-cloud company (D-CSP). The job of E-CSP would be to perform outsourced file encryption operation and D-CSP would be to perform outsourced understanding operation. Within the file encryption phase, the operation connected using the dummy attribute is conducted in your area as the operation connected using the sub-tree is outsourced to E-CSP. Benefits of suggested system: Lessen the heavy computation burden on users. We delegate the majority of computation load to E-CSP and D-CSP and then leave really small computation cost to local devices.

Fundamental Statements: We are saying that DCDH assumption holds if no probabilistic polynomial time (PPT) adversaries can solve the DCDH trouble with for the most part a minimal advantage. The formula outputs a cipher text so that just the user whose attribute set satisfies the access policy can decrypt. Proxy re-file encryption enables a genuine-but-curious proxy to transform a cipher text encrypted by Alice's public key right into a new cipher text that's able tube decrypted by Bob's secret key. Within our Club penguin-ABE plan with user revocation, we think that a user's private key includes a double edged sword. The first is connected together with his approved attributes and yet another the first is connected using the group that they is associated with. Within our security model, the revoked users may collude using the existing users within the same group to fight this group and get use of some data [6]. On the other hand, existing users can get private keys that don't fulfill the specific access structure however the version may be the current version.

Framework: Each interior node within the access tree is really a threshold gate and also the leave nodes are connected with attributes. A person can decrypt a cipher-text only when his attribute set satisfies the access tree baked into the cipher text. The understanding operation contains two steps. The initial step is the fact that D-CSP performs partial understanding. The 2nd step is the fact that DU decrypts mediate leads to get plaintext. In the following paragraphs, we provided a proper definition and security model for Club penguin-ABE with user revocation. We create a concrete Club penguin-ABE plan that is CPA

secure according to DCDH assumption. To face up to collusion attack, we embed certificates in to the user's private key. To ensure that malicious users and also the revoked users don't be capable of produce a valid private key through mixing their private keys. When DO promises to upload his files to CSS and share all of them with you of the specified group, he first defines an access tree and will get the audience public key. During decrypting process, there are plenty of bilinear pairing operations that are computationally costly. To lessen the computation cost, we delegate the pairing operations to D-CSP, around the condition the data submissions are still protected against being uncovered. The primary issue within our plan would be to withstand the collusion attack between your revoked users and existing users [7]. With the introduction of cloud-computing, outsourcing data to cloud server attracts plenty of attentions. To be sure the security and get flexibly fine-grained file access control, attribute based file encryption (ABE) was suggested and utilized in cloud storage system. Furthermore, we delegate operations rich in computation cost to E-CSP and D-CSP to lessen the user's computation burdens. Through using the manner of delegate, computation cost for local devices is a lot lower and comparatively fixed. The outcomes in our experiment reveal that our plan is efficient for resource restricted devices.

4. CONCLUSION:

Our plan is efficient for resource restricted devices for example cell phones. Our plan may be used in cloud storage system that needs the skills of user revocation and fine-grained access control. To lessen users' computation burdens, we introduce two cloud providers named file encryption-cloud company (E-CSP) and understanding-cloud company (D-CSP). The job of E-CSP would be to perform outsourced file encryption operation and D-CSP would be to perform outsourced understanding operation. However, user revocation may be the primary issue in ABE schemes. In the following paragraphs, we offer a cipher text-policy attribute based file encryption (Club penguin-ABE) plan with efficient user revocation for cloud storage system. Thinking about our plan resists collusion attack done by the revoked users cooperating with existing users as the plan doesn't, our plan is much more practical.

REFERENCES:

[1] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han, Member, IEEE, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", IEEE Transactions on Services Computing, 2016.

[2] M. Yang, F. Liu, J. Han, and Z. Wang, "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control," Proc.2011International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 516-520, 2011.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based En-cryption for Fine-Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.

[4] M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryption of ABE ciphertexts,"Proc.20th USENIX Conference on Security (SEC '11), pp. 34, 2011.

[5] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, "Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles,"Proc.16th European Symposium on Research in Computer Security(ESORICS '11), LNCS6879, Berlin:Springer-Verlag, pp. 278-297, 2011.

[6] M. Blaze, G. Bleumerand M. Strauss, "Divertible Protocols and Atom-ic Proxy Cryptography,"Proc.International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '98), LNCS1403, and Berlin: Springer-Verlag, pp. 127-144, 1998.

[7] J.W. Li, C.F. Jia, J. Liand X.F. Chen, "Outsourcing Encryption of At-tribute-Based Encryption with Mapreduce,"Proc.14th International ConferenceonInformation and Communications Security (ICICS '12), LNCS7618, Berlin: Springer-Verlag, pp. 191-201, 2012.

UTILIZE LOCATION IN TURN TO SENSE RINGS AUTHENTICITY REPLICA HIT

Prasad, B[1]., O.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 (✉ plavanya@gmail.com)

2, 3, 4, 5 B.Tech III Year CSE, (16RG1A0567, 16RG1A0584, 16RG1A05B0, 16RG1A0571),

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

ABSTRACT: ***Using the clone recognition protocol, we are designed for maximizing the clone recognition probability. Our objective would be to propose a distributed clone recognition protocol with random witness selection to be able to increase the clone recognition probability as the negative impact of network lifetime and the advantages of data buffer storage ought to be minimized. The ring structure facilitates energy-efficient data forwarding across the path for the witnesses and also the sink. We theoretically prove the suggested protocol is capable of 100 % clone recognition probability with trustful witnesses. Particularly, we exploit the place information of sensors and at random select witnesses situated in a diamond ring place to verify the authenticity of sensors and also to report detected clone attacks. Furthermore, in many existing clone recognition protocols with random witness selection plan, the needed buffer storage of sensors is generally determined by the node density. Extensive simulations show our suggested protocol is capable of lengthy network lifetime by effectively disbursing the traffic load over the network. The present system doesn't make certain that a minimum of one from the witnesses can look into the identity from the sensor nodes to find out whether there's a clone attack or otherwise. The performance from the ERCD protocol is evaluated when it comes to clone recognition probability, power consumption, network lifetime, and knowledge buffer capacity. Extensive simulation results show our suggested ERCD protocol is capable of superior performance with regards to the clone recognition probability and network lifetime with reasonable data buffer capacity.***

Keywords: Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime.

1. INTRODUCTION:

In WSNs, since wireless sensor nodes are often operated by batteries, it is advisable to assess the energy use of sensor nodes and to make sure that normal network operations won't be damaged lower by node outage. Our analysis within these jobs is generic, which may be put on various energy models. Within this paper, we advise a power-efficient location-aware clone recognition protocol in densely deployed WSNs, which could guarantee effective clone attack recognition and keep acceptable network lifetime. For cost-effective sensor placement, sensors are often not tamper-proof devices and therefore are deployed in places without monitoring and protection, causing them to be vulnerable to different attacks. Because of the inexpensive for sensor duplication and deployment, clone attacks have grown to be probably the most critical security issues in WSNs. Thus, it is important to effectively identify clone attacks to guarantee healthy operation of WSNs. To permit efficient clone recognition, usually, some nodes are selected, that are known as witnesses, to assist approve the authenticity from the nodes within the network [1]. When the nodes within the network really want to transmit data, it first transmits the request towards the witnesses for authenticity verification, and witnesses will report a detected attack when the node fails the certification. To attain effective clone recognition, witness selection and authenticity verification should fulfill two needs: witnesses ought to be at random selected and a minimum of among the witnesses can effectively receive all of the verification message(s) for clone recognition. Therefore, the look criteria of clone recognition protocols for sensor systems shouldn't only ensure the high end of clone recognition probability but additionally think about the energy and memory efficiency of sensors. Generally, to ensure effective clone recognition, witnesses have to record source nodes' personal data and approve the authenticity of sensors in line with the stored personal data. In many existing clone recognition protocols, the needed buffer storage size depends upon the network node density, i.e., sensors require a large buffer to record the exchanged information among sensors inside a high-density WSN, and therefore the needed buffer size scales using the network node density. Such requirement helps make the existing protocols not too appropriate for densely-deployed WSNs. Most existing approaches can enhance the effective clone recognition at the fee for energy consumption and memory storage, which might not be appropriate for many sensor systems with limited energy

resource and memory storage. Within this paper, aside from the clone recognition probability, we consider energy consumption and memory storage in the style of clone recognition protocol. We further extend the job by staring at the clone recognition performance with untruthful witnesses and reveal that the clone recognition probability still approaches 98 percent when 10 % of witnesses are compromised. Our protocol is relevant to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to produce attacks. The ERCD protocol could be split into two stages: witness selection and authenticity verification. In witness selection, the origin node transmits its personal data to some witnesses that are at random selected through the mapping function. Within the authenticity verification, verification message across the personal data from the source node is transmitted to the witnesses [2]. As a result, to possess a comprehensive study from the ERCD protocol, we extend the analytical model by evaluating the needed data buffer of ERCD protocol by including experimental leads to support our theoretical analysis. First, we theoretically prove our suggested clone recognition protocol is capable of probability 1 according to trustful witnesses. Second, to judge the performance of network lifetime, we derive the expression of total energy consumption, after which compare our protocol with existing clone recognition protocols. Finally, we derive the expression from the needed data buffer by utilizing ERCD protocol, and reveal that our suggested protocol is scalable since the needed buffer storage relies upon the ring size only.

2. CLASSICAL MODEL:

To permit efficient clone recognition, usually, some nodes are selected, that are known as witnesses, to assist approve the authenticity from the nodes within the network. The non-public information from the source node, i.e., identity and also the location information, are distributed to witnesses in the stage of witness selection. When the nodes within the network really want to transmit data, it first transmits the request towards the witnesses for authenticity verification, and witnesses will report a detected attack when the node fails the certification. To attain effective clone recognition, witness selection and authenticity verification should fulfill two needs: 1) witnesses ought to be at random selected and a pair of) a minimum of one from the witnesses can effectively receive all of the verification message(s) for clone recognition. Randomized Efficient and Distributed protocol (RED) and Line-Select Multicast protocol (LSM) consume their batteries because of the unbalanced energy consumption, and dead sensors could cause network partition, which might further modify the normal operation of WSNs [3]. Disadvantages of existing system: Is to really make it hard for malicious users eavesdrop the communication between current source node and it is witnesses, to ensure that malicious users cannot generate duplicate verification messages. Doesn't guarantee a higher clone recognition probability, i.e., the probability that clone attacks could be effectively detected, it is important and difficult to fulfill these needs in clone recognition protocol design. The look criteria of clone recognition protocols for sensor systems shouldn't only ensure the high end of clone recognition probability but additionally think about the energy and memory efficiency of sensors. The very first occurrence of the sensor that has no energy, it is advisable to not just minimize the power use of each node but additionally balance the power consumption among sensors distributive situated in different regions of WSNs.

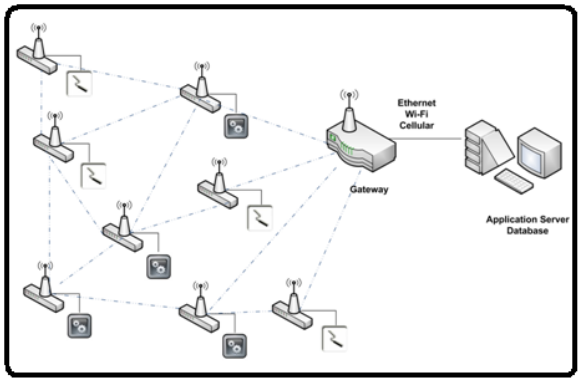


Fig.1.System Framework

3. EFFICIENT DETECTION METHOD:

Within this paper, aside from the clone recognition probability, we consider energy consumption and memory storage in the style of clone recognition protocol, i.e., a power- and memory-efficient distributed clone recognition protocol with random witness selection plan in WSNs. Our protocol is relevant to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to produce attacks. We extend the analytical model by evaluating the needed data buffer of ERCD protocol by including experimental leads to support our theoretical analysis. Energy-Efficient Ring Based Clone Recognition (ERCD) protocol. We discover the ERCD protocol can balance the power use of

sensors at different locations by disbursing the witnesses throughout WSNs except non-witness rings, i.e., the adjacent rings round the sink that ought to not have access to witnesses. Next, we have the perfect quantity of non-witness rings in line with the purpose of energy consumption. Finally, we derive the expression from the needed data buffer by utilizing ERCD protocol, and reveal that our suggested protocol is scalable since the needed buffer storage relies upon the ring size only [4]. Benefits of suggested system: The experiment results show the clone recognition probability can carefully approach 100 % with untruthful witnesses. By utilizing ERCD protocol, energy use of sensors near to the sink has lower traffic of witness selection and authenticity verification, which will help to balance the uneven energy use of data collection.

Proper Plan: We make use of the sink node because the origin from the system coordinator. According to the position of the BS, the network region is actually broken into adjacent rings, in which the width of every ring is equivalent to the transmission selection of sensor nodes. The network model can be extended in to the situation of multiple BSs, where different BSs use orthogonal frequency-division multiple use of communication using its sensor nodes. To manage to performing authenticity verification, every sensor has got the same buffer storage ability to keep information. Buffer storage capacity ought to be sufficient to keep the non-public information of source nodes, so that any node could be selected like a witness. Within our network, the hyperlink level security could be guaranteed by using a standard bootstrapping cryptography plan, and also the sink node utilizes an effective cryptography plan, which can't be compromised by malicious users. All nodes share their ID information along with other nodes within the network. Initially, the sink node broadcasts the content, which notifies the receivers the message originates from index . All nodes, which get the message, will update their ring index to at least one and rebroadcast the content for their neighbors. A malicious user has got the capacity to compromise some sensor nodes found at arbitrary locations. Using the personal data of compromised nodes, a lot of cloned nodes could be generated and deployed in to the network through the malicious user [5]. However, we guess that malicious users cannot compromise nearly all sensor nodes, since no protocol can effectively identify the clone attack with little legitimate sensor nodes. Within this paper, we concentrate on designing a distributed clone recognition protocol with random witness selection by jointly thinking about clone recognition probability, network lifetime and knowledge buffer storage. Initially, a little group of nodes are compromised through the malicious users.

Implementation: Within the authenticity verification, a verification request is distributed in the source node to the witnesses, containing the non-public information from the source node. Initially, network region is actually split into h adjacent rings, where each ring includes a sufficiently many sensor nodes to forward across the ring and also the width of every ring is r. particularly, we've suggested ERCD protocol, including the witness selection and authenticity verification stages. The ERCD protocol includes two stages: witness selection and authenticity verification. In witness selection, an arbitrary mapping function is utilized to assist each source node at random select its witnesses. Additionally, our protocol is capable of better network lifetime and total energy consumption with reasonable storage capacity of information buffer. In WSNs, since wireless sensor nodes are often operated by batteries, it is advisable to assess the energy use of sensor nodes and to make sure that normal network operations won't be damaged lower by node outage. Our analysis within these jobs is generic, which may be put on various energy models. To simplify the outline, we use hop length to represent the minimal quantity of hops within the paper. Because we think about a densely deployed WSN, hop entire network may be the quotient from the distance in the sink towards the sensor in the border of network region within the transmission selection of each sensor. The ERCD protocol begins with a breadth-first search through the sink node to initiate the ring index, and all sorts of neighboring sensors periodically exchange the relative location and ID information. Next, each time a sensor node establishes an information transmission to other people, it must run the ERCD protocol. In witness selection, a diamond ring index is at random selected through the mapping function as witness ring of node. Within the authenticity verification, node a transmits a verification message including its personal data following a same path for the witness ring as with witness selection [6]. To boost the probability that witnesses can effectively get the verification message for clone recognition, the content is going to be broadcast when it's

not far from the witness ring, namely three-ring broadcasts. Each of our theoretical analysis and simulation results have shown our protocol can identify the clone attack with almost probability 1, because the witnesses of every sensor node is shipped inside a ring structure that makes it easy be performed by verification message. Within this paper, we've suggested distributed energy-efficient clone recognition protocol with random witness selection. In distributed clone recognition protocol with random witness selection, the clone recognition probability generally describes whether witnesses can effectively get the verification message in the source node or otherwise. In ERCD protocol, the verification message is broadcast when it's close to the witness ring.

4. CONCLUSION:

The sensors nodes within the transmission route although not found in the witness ring are known as the transmitters. The performance from the ERCD protocol is evaluated when it comes to clone recognition probability, power consumption, network lifetime, and knowledge buffer capacity. It is because we make use of the location information by disbursing the traffic load throughout WSNs, so that the power consumption and memory storage from the sensor nodes round the sink node could be relieved and also the network lifetime could be extended. To find out whether there's a clone attack or otherwise, all of the verification messages received by witnesses are given to the witness header across the same route in witness selection. To boost the probability that witnesses can effectively get the verification message for clone recognition, the content is going to be broadcast when it's not far from the witness ring, namely three-ring broadcasts. Each of our theoretical analysis and simulation results have shown our protocol can identify the clone attack with almost probability 1, because the witnesses of every sensor node is shipped inside a ring structure that makes it easy be performed by verification message. Within our future work, we'll consider different mobility patterns under various network scenarios.

REFERENCES:

[1] Zhongming Zheng, Student Member, IEEE, Anfeng Liu, Member, IEEE, Lin X. Cai, Member, IEEE,Zhigang Chen, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, "Energy and Memory Efficient Clone Detectionin Wireless Sensor Networks", ieee transactions on mobile computing, vol. 15, no. 5, may 2016.

[2] J. Li, J. Chen, and T. H. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors," in Proc. IEEE INFOCOM, Orlando, FL, USA, Mar. 25-30, 2012, pp. 118–126.

[3] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proc. IEEE 17th Int. Conf. Netw. Protocols, Princeton, NJ, USA, Oct. 13-16, 2009, pp. 284–293.

[4] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emergingmachine to machine communications," IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012.

[6] C. Ok, S. Lee, P. Mitra, and S. Kumara, "Distributed routing in wireless sensor networks using energy welfare metric," Inf. Sci., vol. 180, no. 9, pp. 1656–1670, May 2010

USING MACHINE LEARNING FOR CROP SELECTION BASED ON MULTIPLE ENVIRONMENTAL FACTORS IN AGRICULTURE

CH.Rajkumar[1]., B.Shruthika[2]., B.Jahnavi[3]., B.Jhansi[4]., B.Priyanka[5].,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS,

✉ chunchurajkumar@gmail.com

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0414, 15RG1A0415, 15RG1A0416, 15RG1A0417), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— India is an agriculture-based economy where the majority of GDP comes from agriculture. In an economy where most of the food produced comes from agriculture, the choice of plants plays a very important role. Given the declining agricultural production and food shortages across the country, also a consequence of poor crop selection and thus an increase in farmer suicides, we propose a method by which to suggest the most suitable crops that The yield can be maximized by summarizing the analysis of all relevant parameters. [2] These parameters can affect the economy, the environment and natural performance. Economic factors such as market prices, demand, etc. They play a very important role in the decision of a crop, as do environmental factors such as precipitation, temperature, soil type and its chemical composition as well as the overall product. Therefore, it is necessary to develop a system that takes into account all the parameters that affect the best selection of plants that can be grown during the season.

Keywords— harvest selection method, harvest sequencing method, WEKA, classification, selection factor.

1. INTRODUCTION

Agriculture plays a very important role when considering the economic growth of a country like India. In one scenario, the crop yield rate is steadily decreasing. There is a need for an intelligent system that can solve the problem of crop yield reduction. It is very complex for farmers to have more than one crop to grow, especially when market prices are unknown [1]. Based on statistics from Wikipedia, the suicide rate of farmers in India was between 1.4 and 1.8 per 100,000 people over a period of 10 years up to 2005. While there were 5,650 farm suicides in 2014, the number exceeded 8,000 in 2015. To overcome this problem, we propose a system that allows crop selection based on economy, environment and yield in order to get the maximum yield for farmers. Farmers will, one by one, help meet the growing demand for food in the country.

The system uses machine learning to make crop predictions and Java as the programming language since Java is the widely accepted experimental language in the field of machine learning. Machine learning uses historical data and information to gain experience and generate a trained classifier by training it on the data. This classifier then makes output predictions. The better the recording of the data set, the more precise the classifier is. Machine learning methods such as regression and classification have been shown to perform better than various statistical models.

2. RELATED WORKS

The forecast of agricultural products plays a very important role in agriculture. Increase net production, plan better and make more profit. [1] Plant selection is therefore a very difficult task when you need to grow more than one crop. Therefore, a plant selection algorithm is developed to decide which crop (s) to grow based on performance during a season. This method also suggests which culture sequence (s)

It should be grown during the growing season for maximum benefit. When all factors are analyzed together using machine learning, we can predict more accurate future values instead of relying on statistical data. [2] Machine learning is an area of artificial intelligence that finds application in a variety of areas, such as: B. Pattern recognition, weather forecasting, games, etc. Agriculture is one of the areas where this technology can be widely used. Plant diseases and yield forecasting, weather forecasting, and smart irrigation are some of the areas of agriculture where machine learning, if used correctly, can be of great help.

The artificial neural network with back propagation has been proposed to better predict crop yield [3]. The use of artificial neural networks in statistical models and harvest simulations provides more precise information and helps to make better decisions. ANN was used to predict crop yield based on several predictor variables; H. Soil type, PH, nitrogen, phosphate, potassium, organic carbon, calcium, manganese, copper, iron, depth, temperature, precipitation, humidity. ANN was viewed with zero, one and two hidden layers. By calculating the MSE

(Root Mean Square Error), an optimal number of hidden layers as well as an optimal number of units in each hidden layer was found.

3. PROPOSED WORK

Based on the harvest selection method described in [1], we present our two harvest selection methods, which represent an extensive work on [1]. The suggested methods are:

I Crop selection method

ii. Culture sequencing method

The price factor is one of the most important factors that play an important role in plant selection. For example, there are two crops and they both produce the same yield, but one crop is cheaper than the other.

3.1 Plant Selection Method

Crop	Precipitation Level	Temperature Range
Rice	100 - 200 mm	16 - 27C
Tea	150 - 250mm	21 - 29C
Wheat	50 - 100mm	14 - 18C
Jute	125 - 175mm	24 - 37C
Maize	60 - 110 mm	14 - 27C
Rubber	225 - 250mm	25 - 34C
Mustard	625 - 1000mm	10 - 25C

Table 1: Plant and precipitation level

The plant selection method refers to a method of selecting plants in a particular season based on various environmental and economic factors for maximum benefit. These factors are rainfall, average temperature, soil type, market prices and demand, etc. This task can be carried out with WEKA classification algorithms . The most important and essential to get accurate results is the choice of features. The more precise the data sets, the better the predictions.

The temperature around 24 ° C is ideal. The record can be viewed as shown in Table 1.

Soil Type	Climate Type
Alluvial, loamy, clayey	hot, moist
Mountain soil (Iron, lime and humus)	mostly summer
alluvial, mixed	winter, temperate
new alluvial, clayey, sandy	hot damp
sub-tropical	hot, moist
lateritic, well-drained, weathered, alluvial, red	mostly humid (80%)
heavy loamy, well drained	sub-topical, frost-[illegible]

Table 2: Soil and Climate type

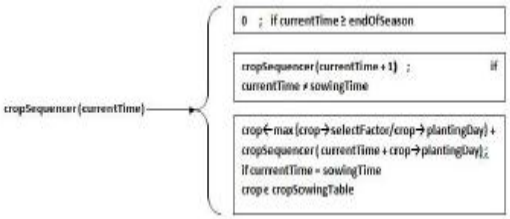
Except for some exceptions, such as the fact that there are various diseases and cultivation errors, or the change in properties observed when using different types of soil. For example, when growing jute on sandy soil, the fiber becomes coarse, while on clay soil it becomes sticky. We made sure of this before proceeding with the crop selection method.

We used WEKA classifiers and regression methods to accurately predict the most suitable plants to grow this season. There are many other traits such as moisture, nutritional value of the soil, pH, etc. that are included in the training dataset, but for the sake of simplicity only the main traits that affect them.

3.2 Plant Sequence Method

The harvest sequencing method uses a harvest sequencing algorithm to suggest the harvest sequence based on the rate of return and market prices. The harvest prices depend heavily on the harvest yields. Therefore, the price of the harvest is one of the most important factors in suggesting the order of harvest based on market prices. Table 2 is a snapshot of the data set used for the culture sequencing method.

Here performance and prices can fluctuate depending on the weather or market conditions. These are just the predicted means that we used for analysis. In the culture sequencing method, we used sets (two or more) of culture (s) as input to our algorithm (the set can be one or more cultures) resulting in a single set. The harvest sequencing algorithm, taking into account the crop yield and prices, suggests exactly the most suitable harvest set to grow throughout the season. Equation 1 explains the algorithm clearly.



Algorithm:

cropSequencer(curentTime)
if currentTime ≥ EndOfSeason then return 0
end if
else if currentTime= sowingTime then return cropSequencer(currentTime + 1)
end if else
cropSowingTable←cropInputTable(currentTime
L: crop ← max{crop →selectFact / crop → plantationDay} crop cropSowingTable
if (currentTime + crop → platationDay) ≥ EndofSeason then
if cropSowingTable is NULL then return cropSowingTable(currentTime + 1) end if else go to L end else end if else
update(OutputcropTable, crop)
npr ← (crop → selectFact + cropSequencer(currentTime + crop →plantationDay)) return npr
end else
end else
end cropSequencer

4 RESULTS

The algorithm explained above is based on the expected return as well as market prices. The "selectFactor" mentioned in the algorithm is the product of the expected return and the current market price of this particular crop. This helps us base our forecasts not only on returns but also on market prices. This is one of the most important metrics used in designing our algorithm. The selection factor for each culture can be different.

Select Factor = Net Yield Rate * Price

Crop	Predicted Yield Rate (kg/hect)	Price (INR/Quintal)
Sugarcane	270	3400-3500
Rice	2000	5200-6200
Soyabean	1264	2700-3000
Potato	1650	2000-2300
Mung	1492	9500 - 9900

Table-2: Dataset for Crop Sequencing Method

5 CONCLUSIONS

Since then, the number of farm suicides has increased day by day. This system can be of great help in predicting crop sequences, as well as in maximizing returns and monetary benefits for farmers. In addition, the successful integration of machine learning into agriculture to predict plant diseases, various irrigation systems, study simulations of plants, etc. This can lead to further advances in agriculture by maximizing yield and optimizing the use of resources.

REFERENCES

1. Miss.Snehal, S.Dahikar, Dr.Sandeep V.Rode, "Agricultural Crop Yield Prediction Using Artificial Neural Network Approach". International Journal of Innovative Reasearch in Electrical, Electronic, Instrumentation and Control Engineering, Vol. 2, Issue 1, January 2014.
2. Thoranin Sujjaviriyasup, "Agricultural Product Forecasting Using Machine Learning Approach". Int. Journal of Math. Analysis, Vol. 7, 2013, no. 38, 1869 – 1875.
3. Rakesh Kumar, M.P. Singh, Prabhat Kumar and J.P. Singh,"Crop Selection Method to Maximize Crop Yield Rate using Machine Learning Technique" 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 6 - 8 May 2015. pp.138-145. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
4. Karandeep Kaur, "Machine Learning: Applications in Indian Agriculture". International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016 .
5. Anastasiya Kolesnikova, Chi-Hwa Song, Won Don Lee, "Applying UChooBoost algorithm in Precision Agriculture". ACM International Conference on Advances in Computing, Communication and Control, Mumbai, India, January 2009.
6. Krishna Kumar, K. Rupa Kumar, R. G. Ashrit, N. R. Deshpande and J. W. Hansen, "Climate Impacts on Indian Agriculture". International Journal of climatology, 24: 13751393, 2004.

SECURITY IMPROVISATION IN CLOUD COMPUTING USING CAPGP AND IMAGE CAPTCHA

N.Uma Maheshwari[1]., E.Pavani[2]., G.Anusha[3]., G.Harika[4]., K.Sushmitha[5].,

1Professor, 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, (15RG1A0435, 15RG1A0436, 15RG1A0441, 15RG1A0468), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The success of the cloud computing paradigm is based on its on-demand, self-service, and consumption nature. According to this paradigm, the impact of denial of service (DoS) attacks affects not only the quality of the service provided, but also the cost of service in terms of resource consumption. The longer the detection time, the higher the cost. Therefore, special attention should be paid to covert DoS attacks. Their purpose is to minimize your visibility, and at the same time, they can be as devastating as brute force attacks. These are sophisticated attacks designed to exploit the lower performance of the target system through specific periodic, bursting, and low-traffic traffic patterns. In this article, we propose a strategy for orchestrating stealthy attack patterns that are gradually increasing in intensity to maximize the financial cost to the cloud client based on the volume of work and the number of workers on the construction site. The arrival of services imposed by discovery mechanisms. We describe both the application of the proposed strategy and its impact on the target system provided in the cloud.

Keywords— cloud computing, sophisticated attack strategy, slow attacks, intrusion detection.

1. INTRODUCTION

Cloud providers offer computer and storage rental services as transparently as possible and create the impression of "unlimited resource availability". These resources are not free. In this way, cloud providers allow customers to properly maintain and tune system capacity and quickly re-evaluate that capacity as their needs change so that customers can only pay for the resources they really need. "They really use them. Some cloud providers offer Load Balancing to automatically distribute incoming App Service requests across multiple instances, as well as Auto Scale so that consumers can accurately monitor the demand curve of their applications. To minimize customer costs, auto-scaling ensures that the number of application instances increases smoothly during peak loads and automatically decreases during demand fluctuations. For example, with Amazon EC2 cloud services, consumers can set a condition to add new compute instances when the average CPU usage exceeds a fixed threshold. You can also configure a cool-down period to allow the application workload to stabilize before adding or removing autoscaler instances. This is how this feature can be maliciously exploited with a stealth attack that can slowly deplete the resources provided by the cloud service provider to ensure SLA and increase costs for the cloud client.

2. LITERATURE REVIEW

In this article, we present a new concept of a policy orchestration service that aims to make it easier to control security and data protection in a company, especially when the company has various services from external providers in the cloud. The orchestration service acts as an intermediary between the company's internal decision support systems (which contain important data protection and security best practices) and the cloud service providers who are to be subject to contractual service level agreements with the company. The role of the orchestration service, which should be accessed as a trusted cloud service, is to ensure that applicable data protection and security guidelines from service providers are auctioned off through appropriate enforcement and control mechanisms [1]. Cloud computing is a new business model that enables users, businesses and public organizations to reduce costs and increase efficiency, and is another way to deliver services and resources. In this pay-as-you-go model, security plays a key role. Cyber attacks pose a serious threat that can affect the quality of services provided to customers, as well as the cost of provided cloud services and resources. This article presents a hierarchical hybrid event correlation approach to cloud intrusion detection. It includes identifying symptoms of theft by collecting a variety of information from different layers of the cloud architecture, using distributed security probes, and performing complex event analysis based on a processing engine. Complex measures. The process of escalating intrusion symptoms to an identified cause and purpose of the intrusion process is

controlled by a knowledge base represented by an ontology. Also presented is a prototype of the proposed solution for intrusion detection [2].

3. EXISTING SYSTEM

Sophisticated DDoS attacks are defined as this category of attacks that are designed to damage a specific weakness in the design of the target system in order to lead to denial of service or simply to significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks. The sophisticated methods of launching attacks fall into two categories: task content and task arrival patterns. In recent years, a variety of DoS attacks have been proposed using low-speed traffic, including stubborn attacks (LDoS), degraded attacks (RoQ), and low-speed DoS attacks on application servers (LoRDAS).
Disadvantage:
1. Sophisticated DDoS attacks are defined as this category of attacks, the purpose of which is to damage a specific weak point in the design of the target system in order to cause denial of service or simply significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks.
2. Sophisticated methods of launching attacks fall into two categories: job content-based and hiring patterns.
3. In recent years, low-speed traffic DoS attacks have been proposed, including Shrew attacks (LDoS), degrading attacks (RoQ), and low-speed DoS attacks on server applications. -Server (LoRDAS).

4. PROPOSED SYSTEM

This article presents a sophisticated stealth attack strategy for cloud-based applications. The proposed strategy is not about making the service unavailable, but about taking advantage of the flexibility of the cloud and making the application consume more resources than necessary, which the cloud client makes more financially than the availability of the service. The attack pattern is organized in such a way as to circumvent the methods proposed in the literature to detect attacks with low performance or for their significant delay. It does not display the periodic waveform typical of low bitrate exhaustive attacks. In contrast, it is an iterative and gradual process. In particular, the attack power (in terms of the speed of service requests and concurrent attack sources) is slowly increased by a patient attacker, resulting in significant financial losses, even if the attack pattern is based on the maximum size and arrival. work. The rate of service requests authorized in the system. Using an empirically developed simplified model, we derive an expression for a gradual increase in attack power depending on the achieved degradation of service quality (without prior knowledge of the target system power). We show that features offered by a cloud service provider to ensure a customer-agreed SLA (including load balancing and autoscaling mechanisms) can be maliciously exploited through a proposed stealth attack that slowly consumes the resources provided by the cloud. The supplier increases the costs borne by the customer. The proposed attack strategy, the Slow-Growing Polymorphic DDoS Attack Strategy (SIPDAS), can be applied to various types of attacks that exploit known application vulnerabilities to compromise a server-provided service. Targeted applications running in the cloud.

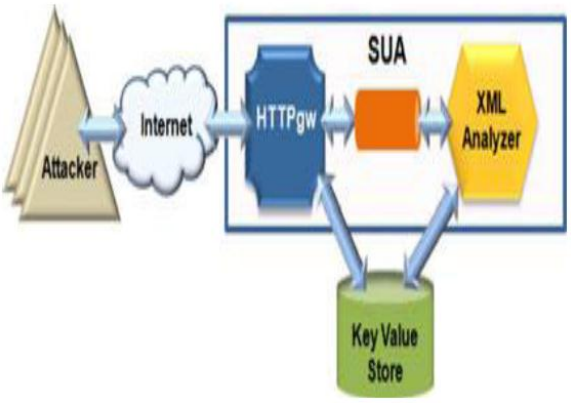


Fig. 1: Functional diagram of the proposed system.

5. DESCRIPTION OF MODULES

A. Server model under attack:
To assess the quality of service degradation associated with an attack, we define a synthetic representation of the attacked system. We assume that the system consists of a group of distributed virtual machines that

are provided by a cloud provider and that run application instances. We also assume that there is a load balancing mechanism that distributes user service requests across instances. The number of instances can be automatically increased or decreased by tracking certain relevant parameters to assess the quality of the services provided (for example, computational load, memory used, and number of active users). Specifically, we simulate an attacked system with total capacity, which is the total amount of work that the system can do to process service requests. This ability is influenced by various parameters, for example. For example, B. number of virtual machines assigned to the application, processing power, storage capacity, etc. Each service request consumes a certain capacity depending on the payload of the service request. Thus, the system load CN at time t can be modeled by a queue system with Poisson arrivals, exponentially distributed service time, multiple servers, and n current incoming requests (system throughput). In addition, cloud autoscaling is modeled in a simple way: when new resources (such as virtual machines) are added to the system, it increases the capacity of the system.

B. Creation of wear in service:

Imagine a cloud-based system with full service request processing capabilities and a B-size queue that represents a common bottleneck for client and DoS flows. Use C0 to indicate the load at the beginning of the attack period T (assuming this is at time t0), and CN as the load to process user requests on the target system during the time window T. destination, the number of threads n must be organized. ...

C. Minimize the visibility of attacks:

According to the previous definition of a covert attack, conditions must be met to reduce the signature of the attack. Hence, the patient and the experienced attacker should be able to detect the application of the vulnerability (for example, a deeply nested XML vulnerability) by scanning both the target system and legitimate service requests (for example, for HTTP messages, including the XML document structure).) and identify the set of types of legitimate service requests that could be exploited to exploit this vulnerability. For example, in an X-DoS attack, an attacker could implement a series of XML messages with a different number of nested tags. The NT threshold can be arbitrarily set, or possibly estimated during a training phase in which an attacker inserts a sequence of messages with an increasing number of nested XML tags to identify a possible threshold-based XML validation constraint. A similar approach can be used to estimate the maximum message rate at which service requests should be inserted.

D. XML-based DoS attack

In a pilot campaign, we analyzed CPU utilization based on the number of nested XML tags and the frequency with which malicious messages were injected. In particular, the CPU consumption on the target system for parsing messages containing XML tags with different nesting depths. [t] Results showed that messages from 500 nested beacons are enough to generate a maximum CPU utilization of about 97%, while with 1000 beacons the processor processes the entire message in about 3 seconds. In addition, we carry out various attacks. For each attack, we introduce a uniform XDoS stream, that is, a sequence of messages with a fixed number of nested tags and a fixed message rate. Let us assume that 20 seconds is the maximum experimentally observed time to reach the stable state value of the attacked processor (ie CR), and denote the "baseline" as the average processor load in the absence of user load (about 9%). There are several ways to implement a SIPDAS based attack. In this work, we use the same cloud framework that we used to create a targeted server application.

6.RESULTS

We demonstrate that the proposed slow-growing polymorphic behavior causes significant overload on the target system (resulting in significant financial losses) and significantly bypasses or delays detection methods. Even if the victim detects an attack, the attack process can be restarted by exploiting another application vulnerability (form polymorphism) or synchronization (time polymorphism) to increase the consumption of extended resources.

7. CONCLUSION

In this article, we propose a strategy for implementing stealth attack schemes that exhibit slowly growing polymorphic behavior that can significantly evade or delay methods proposed in the literature for detecting underperforming attacks. By exploiting a vulnerability in the target application, a patient and a smart attacker can coordinate complex message flows that can be distinguished from legitimate service requests. Specifically, the proposed attack model seeks

to take advantage of the flexibility of the cloud, rather than making the service unavailable and forcing the services to scale and consume more resources than necessary, making the cloud client more financial than when it comes to a service issue availability.

REFERENCES

1. H. Sun, J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proc. 12th IEEE Int. Conf. Netw. Protocol., 2004, pp. 196-205.
2. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.
3. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.
4. M. Ficco, "Security event correlation approach for cloud computing," Int. J. High Perform. Comput. Netw., vol. 7, no. 3, pp. 173–185, 2013.
5. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.
6. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

DENIAL OF SERVICE IN CLOUD COMPUTING: A SURVEY ON SOPHISTICATED ATTACK STRATEGY

Dr. Archek praveen kumar[1]., R.Vani[2]., R.Radhika[3]., R.Meghana[4]., S.Nandhini[5].,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ archekpraveen@mrcew.ac.in)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A04B2, 15RG1A04B3, 15RG1A04B4, 15RG1A04B5), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— The success of the cloud computing paradigm is based on its on-demand, self-service, and consumption nature. According to this paradigm, the impact of denial of service (DoS) attacks affects not only the quality of the service provided, but also the cost of service in terms of resource consumption. The longer the detection time, the higher the cost. Therefore, special attention should be paid to covert DoS attacks. Their purpose is to minimize your visibility, and at the same time, they can be as devastating as brute force attacks. These are sophisticated attacks designed to exploit the lower performance of the target system through specific periodic, bursting, and low-traffic traffic patterns. In this article, we propose a strategy for orchestrating stealthy attack patterns that are gradually increasing in intensity to maximize the financial cost to the cloud client based on the volume of work and the number of workers on the construction site. The arrival of services imposed by discovery mechanisms. We describe both the application of the proposed strategy and its impact on the target system provided in the cloud.

Keywords*— cloud computing, sophisticated attack strategy, slow attacks, intrusion detection.

1. INTRODUCTION

Cloud providers offer computer and storage rental services as transparently as possible and create the impression of "unlimited resource availability". These resources are not free. In this way, cloud providers allow customers to properly maintain and tune system capacity and quickly re-evaluate that capacity as their needs change so that customers can only pay for the resources they really need. "They really use them. Some cloud providers offer Load Balancing to automatically distribute incoming App Service requests across multiple instances, as well as Auto Scale so that consumers can accurately monitor the demand curve of their applications. To minimize customer costs, auto-scaling ensures that the number of application instances increases smoothly during peak loads and automatically decreases during demand fluctuations. For example, with Amazon EC2 cloud services, consumers can set a condition to add new compute instances when the average CPU usage exceeds a fixed threshold. You can also configure a cool-down period to allow the application workload to stabilize before adding or removing autoscaler instances. This is how this feature can be maliciously exploited with a stealth attack that can slowly deplete the resources provided by the cloud service provider to ensure SLA and increase costs for the cloud client.

2. LITERATURE REVIEW

In this article, we present a new concept of a policy orchestration service that aims to make it easier to control security and data protection in a company, especially when the company has various services from external providers in the cloud. The orchestration service acts as an intermediary between the company's internal decision support systems (which contain important data protection and security best practices) and the cloud service providers who are to be subject to contractual service level agreements with the company. The role of the orchestration service, which should be accessed as a trusted cloud service, is to ensure that applicable data protection and security guidelines from service providers are auctioned off through appropriate enforcement and control mechanisms [1].

Cloud computing is a new business model that enables users, businesses and public organizations to reduce costs and increase efficiency, and is another way to deliver services and resources. In this pay-as-you-go model, security plays a key role. Cyber attacks pose a serious threat that can affect the quality of services provided to customers, as well as the cost of provided cloud services and resources. This article presents a hierarchical hybrid event correlation approach to cloud intrusion detection. It includes identifying symptoms of theft by collecting a variety of information from different layers of the cloud architecture, using distributed security probes, and performing complex event analysis based on a processing engine. Complex measures. The process of escalating intrusion symptoms to an identified cause and purpose of the intrusion process is controlled by a knowledge base represented by an ontology.

Also presented is a prototype of the proposed solution for intrusion detection [2].

3. EXISTING SYSTEM

Sophisticated DDoS attacks are defined as this category of attacks that are designed to damage a specific weakness in the design of the target system in order to lead to denial of service or simply to significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks. The sophisticated methods of launching attacks fall into two categories: task content and task arrival patterns. In recent years, a variety of DoS attacks have been proposed using low-speed traffic, including stubborn attacks (LDoS), degraded attacks (RoQ), and low-speed DoS attacks on application servers (LoRDAS).

Disadvantage:

1. Sophisticated DDoS attacks are defined as this category of attacks, the purpose of which is to damage a specific weak point in the design of the target system in order to cause denial of service or simply significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks.
2. Sophisticated methods of launching attacks fall into two categories: job content-based and hiring patterns.
3. In recent years, low-speed traffic DoS attacks have been proposed, including Shrew attacks (LDoS), degrading attacks (RoQ), and low-speed DoS attacks on server applications. -Server (LoRDAS).

4. PROPOSED SYSTEM

This article presents a sophisticated stealth attack strategy for cloud-based applications. The proposed strategy is not about making the service unavailable, but about taking advantage of the flexibility of the cloud and making the application consume more resources than necessary, which the cloud client makes more financially than the availability of the service. The attack pattern is organized in such a way as to circumvent the methods proposed in the literature to detect attacks with low performance or for their significant delay. It does not display the periodic waveform typical of low bitrate exhaustive attacks. In contrast, it is an iterative and gradual process. In particular, the attack power (in terms of the speed of service requests and concurrent attack sources) is slowly increased by a patient attacker, resulting in significant financial losses, even if the attack pattern is based on the maximum size and arrival. work. The rate of service requests authorized in the system. Using an empirically developed simplified model, we derive an expression for a gradual increase in attack power depending on the achieved degradation of service quality (without prior knowledge of the target system power). We show that features offered by a cloud service provider to ensure a customer-agreed SLA (including load balancing and autoscaling mechanisms) can be maliciously exploited through a proposed stealth attack that slowly consumes the resources provided by the cloud. The supplier increases the costs borne by the customer. The proposed attack strategy, the Slow-Growing Polymorphic DDoS Attack Strategy (SIPDAS), can be applied to various types of attacks that exploit known application vulnerabilities to compromise a server-provided service. Targeted applications running in the cloud.

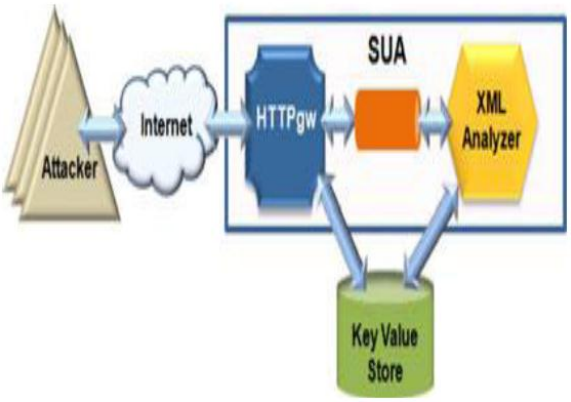


Fig. 1: Functional diagram of the proposed system.

5. DESCRIPTION OF MODULES

A. Server model under attack:

To assess the quality of service degradation associated with an attack, we define a synthetic representation of the attacked system. We assume that the system consists of a group of distributed virtual machines that are provided by a cloud provider and that run application instances. We also assume that there is a load balancing mechanism that distributes user service requests across instances. The number of instances can be automatically increased or decreased by

tracking certain relevant parameters to assess the quality of the services provided (for example, computational load, memory used, and number of active users). Specifically, we simulate an attacked system with total capacity, which is the total amount of work that the system can do to process service requests. This ability is influenced by various parameters, for example. For example, B. number of virtual machines assigned to the application, processing power, storage capacity, etc. Each service request consumes a certain capacity depending on the payload of the service request. Thus, the system load CN at time t can be modeled by a queue system with Poisson arrivals, exponentially distributed service time, multiple servers, and n current incoming requests (system throughput). In addition, cloud autoscaling is modeled in a simple way: when new resources (such as virtual machines) are added to the system, it increases the capacity of the system.

B. Creation of wear in service:

Imagine a cloud-based system with full service request processing capabilities and a B-size queue that represents a common bottleneck for client and DoS flows. Use C0 to indicate the load at the beginning of the attack period T (assuming this is at time t0), and CN as the load to process user requests on the target system during the time window T. destination, the number of threads n must be organized. ...

C. Minimize the visibility of attacks:

According to the previous definition of a covert attack, conditions must be met to reduce the signature of the attack. Hence, the patient and the experienced attacker should be able to detect the application of the vulnerability (for example, a deeply nested XML vulnerability) by scanning both the target system and legitimate service requests (for example, for HTTP messages, including the XML document structure).) and identify the set of types of legitimate service requests that could be exploited to exploit this vulnerability. For example, in an X-DoS attack, an attacker could implement a series of XML messages with a different number of nested tags. The NT threshold can be arbitrarily set, or possibly estimated during a training phase in which an attacker inserts a sequence of messages with an increasing number of nested XML tags to identify a possible threshold-based XML validation constraint. A similar approach can be used to estimate the maximum message rate at which service requests should be inserted.

D. XML-based DoS attack

In a pilot campaign, we analyzed CPU utilization based on the number of nested XML tags and the frequency with which malicious messages were injected. In particular, the CPU consumption on the target system for parsing messages containing XML tags with different nesting depths. [t] Results showed that messages from 500 nested beacons are enough to generate a maximum CPU utilization of about 97%, while with 1000 beacons the processor processes the entire message in about 3 seconds. In addition, we carry out various attacks. For each attack, we introduce a uniform XDoS stream, that is, a sequence of messages with a fixed number of nested tags and a fixed message rate. Let us assume that 20 seconds is the maximum experimentally observed time to reach the stable state value of the attacked processor (ie CR), and denote the "baseline" as the average processor load in the absence of user load (about 9%). There are several ways to implement a SIPDAS based attack. In this work, we use the same cloud framework that we used to create a targeted server application.

6.RESULTS

We demonstrate that the proposed slow-growing polymorphic behavior causes significant overload on the target system (resulting in significant financial losses) and significantly bypasses or delays detection methods. Even if the victim detects an attack, the attack process can be restarted by exploiting another application vulnerability (form polymorphism) or synchronization (time polymorphism) to increase the consumption of extended resources.

7. CONCLUSION

In this article, we propose a strategy for implementing stealth attack schemes that exhibit slowly growing polymorphic behavior that can significantly evade or delay methods proposed in the literature for detecting underperforming attacks. By exploiting a vulnerability in the target application, a patient and a smart attacker can coordinate complex message flows that can be distinguished from legitimate service requests. Specifically, the proposed attack model seeks to take advantage of the flexibility of the cloud, rather than making the service unavailable and forcing the services to scale and consume more resources than necessary, making the cloud client more financial than when it comes to a service issue availability.

REFERENCES

1. H. Sun, J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proc. 12th IEEE Int. Conf. Netw. Protocol., 2004, pp. 196-205.
2. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.
3. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.
4. M. Ficco, "Security event correlation approach for cloud computing," Int. J. High Perform. Comput. Netw., vol. 7, no. 3, pp. 173–185, 2013.
5. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.
6. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

CROSS DOMAIN RECOMMENDER SYSTEM AND TRADA ALGORITHM IN MACHINE LEARNING

Dr. Selvamani indrajith[1]., K.Jahnavi [2]., K.Krishnapriya [3]., K.Pushpa[4]., K.Vasavi [5].,

1Professor, 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, (15RG1A0459, 15RG1A0445, 15RG1A0429, 15RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Useful knowledge from the secondary domain can be transferred to the target domain via the social domain. However, there can sometimes be problems with cold starting items in the target domain. To solve this problem, we apply a cross-domain algorithm with a page ranking algorithm. The cross-domain algorithm is divided into two stages. In the first step, we use the TrAda Boost algorithm to select specific items that are recommended to users in the target domain. In the second step, we apply a grouping algorithm for nonparametric pairs to decide if the user is a recommended member or not. The algorithm determines the recommended or not recommended groups of buyers for the article in two stages. We then use a page ranking algorithm to provide users with relevant and unsolicited data.

Keywords— : collaborative filtering, cross-domain, nonparametric pairwise clustering algorithm, impulse TrAda algorithm.

1. INTRODUCTION

Recommender systems have been an important area of research since the first articles on collaborative filtering appeared in the mid-1990s. [4] [5] [6] There have been many developments in the industry and industry over the past ten years. a lot of scientific work in the direction of new approaches to systemic recommendations. Interest in this area remains high as it is a problematic area of research and many practical applications that help users cope with information overload and provide them with recommendations, personalized content and services. [3]. A social network is a platform that allows users to create and use different types of items, such as posts, data, or images. This huge volume of articles poses the problem of information overload. [2] With the development of information technology, we have already entered the era of big data. However, it is important to identify effective data in different areas. [7] Most recommender systems have problems with cold start. The cold start problem concerns not only a new inexperienced user, but also a new subject with low qualifications and a complete system.

1.1 Cross-domain:

A cross-domain method is an information security tool that can be used to manually or automatically access or transfer information between two or more different security domains. They are integrated systems of hardware and software that allow information to be passed between conflicting security domains or classification levels.

The goal of a cross-domain system is to allow an isolated, mission-critical network to communicate with others without posing the security threat that network connectivity typically poses. It consists of three main elements:

1. Data confidentiality
2. Data integrity
3. Data availability

1.2 System of recommendations:

Recommender systems, or recommendation systems, are a subclass of information filtering systems that attempt to predict the "rating" or "preference" that a user would give to an article. Recommender systems typically create a recommendation list in two ways: content-based and collaborative filtering, or individualized.

2. RELATED WORK

Collaborative filtering:

Collaborative filtering is a method of automatically predicting (filtering) the interests of a user by collecting preferences or information about what many users like (jointly). Many company websites use referral systems to help customers find products and content. Modern recommendations are based on collaborative filtering — they use learned patterns of user behavior to make recommendations, usually in the form of lists of related items.

The Proposed System

In this section, we describe the proposed system architecture and our two-step algorithm: first, the TrAdaBoost algorithm is used to filter out invalid data and generate random items that should be recommended to users, and then it becomes a second step, not a parametric Paired Grouping algorithm was applied to group users into two groups based on the recommended item from the first step.

In addition, we use a page ranking algorithm in which the PageRank of a page is determined recursively and depends on the PageRank amount and the scores of all the pages that link to it ("inbound links"), and we leave this data content unexplored. and relevant.

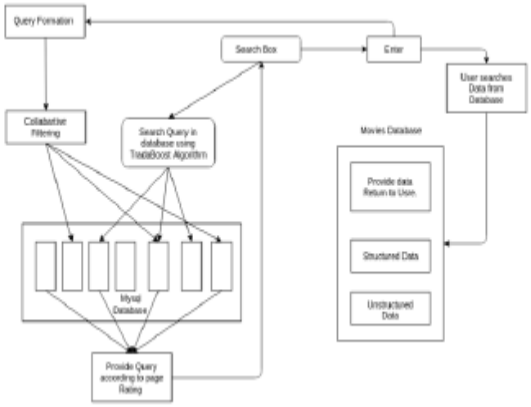


Fig: TrAdaBoost algorithm

It can be used in conjunction with many other types of learning algorithms to improve performance. The result of other learning algorithms ("weak learners") is combined into a weighted sum, which is the final result of the extended classifier. AdaBoost is adaptive in the sense that later weak learners are modified in favor of instances that were misclassified by earlier classifiers.

AdaBoost is sensitive to noisy data and outliers. For some problems, it may be less sensitive to the overfitting problem than other learning algorithms. Individual students may be weak, but as long as the overall performance is slightly better, it will be possible to show random assumptions that the late model converges for the strong student.

Algorithm 1: TrAdaBoost

Input: Two data records labeled Ds and Dt_test lead to a data record without the Dt_test label.

Output: sets the maximum number of iterations M; and define the initial vector of weights W1 = (W11,..., W1n + m).

Loop:

For i = 1…. NOT

1.Set

$$p^t = w^t / \left(\sum_{i=1}^{n+m} W_i^t\right)$$

pt = weight / ()

2. Invoke the student and enter the distribution of pt over X and the unlabeled dataset Dt_test into the training set X. Then reconstruct the ht: X -> Y (or [0,1] guess to be sure);

3. Calculate the error ht in the train Dt_:

$$\beta_i = err_i/(1 = err_i);$$

$$\beta - 1/(1 + \sqrt{2Ln\, n/N};$$

4. Set

$$err_i = \sum_{i-n+1}^{n+m} \frac{W_i^t\,|h_t(x) - c(x_t)|}{\sum_{i-n+1}^{n+m} W_i^t}$$

Moreover, the error should be less than half.

5. Update the new weight vector.

$$W_i^{t+1} = \begin{cases} W_i^t\, \beta_t^{|h_t(x_i)-c(x_i)|} \\ W_i^t\, \beta_t^{-|h_t(x_i)-c(x_i)|} \end{cases}$$

Output: The Hypothesis,

Page Ranking algorithm:

PageRank is a link analysis algorithm that assigns a numerical weight to each item in a series of hypertext documents, such as the World Wide Web, to "measure" their overall relative importance. The algorithm can be applied to any collection of cited and referenced entities. The numerical weight assigned to a particular element E is called PageRank E and is known as PR (E).

Grouping by nonparametric pair:

Nonparametric pairwise clustering helps us group data without specifying specific parameters. When grouping, similarity conditions between data points are taken into account for grouping purposes. In two nonparametric classifiers, i.e. H. Nearest Neighbor (NN) classifier and complement classifier (or kernel density classifier). The generalization error limits for two ignored classifiers are expressed as the sum of paired terms pair

Input: First phase output {I1 ..... Ip} and D.

Initialization: determine the maximum points closest to Ij m, the user size k (U1 ..... Uk) and the maximum number of iterations N.

1) Find the m nearest neighbors Ij and put them = {Ij, I1, ... In} and we assume that U0 should be recommended as a more suitable virtual user.

2) For each user D, let U0i = U0 ∩ Ui (I = 1… k, k is the size of randomly selected users in D) is the vector of insertion of elements, which is U0 for all other users.

3) Calculate the proximity (distance) from point U0i to all other points:

di = (di1, di2, ... dick).

4) Iteration

For t = 1, ... N.

Normalization phase. Normalize di by separating each of its components with || split di ||.
Hence the resulting normalized vector will be

$$\frac{d_{i1}}{||d_i||} \ldots\ldots \frac{d_{ik}}{||d_i||}$$

Pi = (pi1, pi2, …… .. pik) =,
Revaluation step. Estimate the closeness between each pair of new data points i and j so that dij = dist (pi, pj).
Completed
Output: The result of array A, which only contains 0s and 1s.

3 CONCLUSIONS

This article discusses collaborative filtering for forecasting. We will also look at the various limitations of the current recommendation method and discuss potential improvements that could provide better recommendation functionality. We have redefined the cold start problem in the target area

4.RESULTS

Transfer knowledge from other supporting areas. Thus, the proposed system reduces the cold start problem by using a cross-domain recommendation algorithm, which is mainly split into two-part TraAdaboost algorithm and nonparametric pairwise clustering. The system filters search results and provides users with relevant search queries.

REFERENCES

1. Panpan Liu,Jingjing Cao, Xiaolei Liang, Wenfeng Li “A Two Stage Cross Domain Recommendation For Cold Start Problem in Cyber-physical System”, 2015.
2. Meng Jiang, Peng Cui, Xumin Chen, Fei Wang, Wenwu Zhu, “Social Recommendation with Cross-Domain Transferable Knowledge”, 2015.
3. P. Resnick, N. Iakovou, M. Sushak, P. Bergstrom, and J. Riedl, “GroupLens: An Open Architecture for Collaborative Filtering of Netnews,” Proc. 1994 Computer Supported Cooperative Work Conf., 1994.
4. U. Shardanand and P. Maes, “Social Information Filtering:Algorithms for Automating ‘Word of Mouth’,” Proc. Conf. Human Factors in Computing Systems, 1995.
5. Rajkumar R R, Lee I, Sha L, “Cyber-physical Systems: The next computing revolution”, Proceedings of 47th Design Automation Conference. ACM, 2010.
6. Zhen H, Hu F, “Cyber-physical System For Smart Grid Applications”, Cyber-physical Systems: Integrated Computing and Engineering Design, 2013.
7. Gediminas Adomavicius, Member, IEEE, and Alexander Tuzhilin, Member, IEEE., “Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions”, 2005.

RELATIVE ANALYSIS AND OVERVIEW OF LOW-COST OPEN SOURCE WEB TESTING SOFTWARE TOOLS

Jyothi, P[1]., K.Mounika [2]., K.Shruthi [3]., K.Manisha [4]., K.Anusha [5].,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ jyothip@mrcew.ac.in)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0458, 15RG1A0459, 15RG1A0461, 15RG1A0462), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The success of the cloud computing paradigm is based on its on-demand, self-service, and consumption nature. According to this paradigm, the impact of denial of service (DoS) attacks affects not only the quality of the service provided, but also the cost of service in terms of resource consumption. The longer the detection time, the higher the cost. Therefore, special attention should be paid to covert DoS attacks. Their purpose is to minimize your visibility, and at the same time, they can be as devastating as brute force attacks. These are sophisticated attacks designed to exploit the lower performance of the target system through specific periodic, bursting, and low-traffic traffic patterns. In this article, we propose a strategy for orchestrating stealthy attack patterns that are gradually increasing in intensity to maximize the financial cost to the cloud client based on the volume of work and the number of workers on the construction site. The arrival of services imposed by discovery mechanisms. We describe both the application of the proposed strategy and its impact on the target system provided in the cloud.

Keywords— cloud computing, sophisticated attack strategy, slow attacks, intrusion detection.

1. INTRODUCTION

Cloud providers offer computer and storage rental services as transparently as possible and create the impression of "unlimited resource availability". These resources are not free. In this way, cloud providers allow customers to properly maintain and tune system capacity and quickly re-evaluate that capacity as their needs change so that customers can only pay for the resources they really need. "They really use them. Some cloud providers offer Load Balancing to automatically distribute incoming App Service requests across multiple instances, as well as Auto Scale so that consumers can accurately monitor the demand curve of their applications. To minimize customer costs, auto-scaling ensures that the number of application instances increases smoothly during peak loads and automatically decreases during demand fluctuations. For example, with Amazon EC2 cloud services, consumers can set a condition to add new compute instances when the average CPU usage exceeds a fixed threshold. You can also configure a cool-down period to allow the application workload to stabilize before adding or removing autoscaler instances. This is how this feature can be maliciously exploited with a stealth attack that can slowly deplete the resources provided by the cloud service provider to ensure SLA and increase costs for the cloud client.

2. LITERATURE REVIEW

In this article, we present a new concept of a policy orchestration service that aims to make it easier to control security and data protection in a company, especially when the company has various services from external providers in the cloud. The orchestration service acts as an intermediary between the company's internal decision support systems (which contain important data protection and security best practices) and the cloud service providers who are to be subject to contractual service level agreements with the company. The role of the orchestration service, which should be accessed as a trusted cloud service, is to ensure that applicable data protection and security guidelines from service providers are auctioned off through appropriate enforcement and control mechanisms [1].

Cloud computing is a new business model that enables users, businesses and public organizations to reduce costs and increase efficiency, and is another way to deliver services and resources. In this pay-as-you-go model, security plays a key role. Cyber attacks pose a serious threat that can affect the quality of services provided to customers, as well as the cost of provided cloud services and resources. This article presents a hierarchical hybrid event correlation approach to cloud intrusion detection. It includes identifying symptoms of theft by collecting a variety of information from different layers of the cloud architecture, using distributed security probes, and performing complex event analysis based on a processing engine. Complex measures. The process of escalating intrusion symptoms to an identified cause and purpose of the intrusion process is controlled by a knowledge base represented by an ontology.

Also presented is a prototype of the proposed solution for intrusion detection [2].

3. EXISTING SYSTEM

Sophisticated DDoS attacks are defined as this category of attacks that are designed to damage a specific weakness in the design of the target system in order to lead to denial of service or simply to significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks. The sophisticated methods of launching attacks fall into two categories: task content and task arrival patterns. In recent years, a variety of DoS attacks have been proposed using low-speed traffic, including stubborn attacks (LDoS), degraded attacks (RoQ), and low-speed DoS attacks on application servers (LoRDAS).

Disadvantage:

1. Sophisticated DDoS attacks are defined as this category of attacks, the purpose of which is to damage a specific weak point in the design of the target system in order to cause denial of service or simply significantly affect performance. The term stealth has been used to refer to sophisticated attacks specifically designed to make malicious behavior virtually invisible to detection mechanisms. These attacks can be much more difficult to detect than more traditional brute force and flood attacks.
2. Sophisticated methods of launching attacks fall into two categories: job content-based and hiring patterns.
3. In recent years, low-speed traffic DoS attacks have been proposed, including Shrew attacks (LDoS), degrading attacks (RoQ), and low-speed DoS attacks on server applications. -Server (LoRDAS).

4. PROPOSED SYSTEM

This article presents a sophisticated stealth attack strategy for cloud-based applications. The proposed strategy is not about making the service unavailable, but about taking advantage of the flexibility of the cloud and making the application consume more resources than necessary, which the cloud client makes more financially than the availability of the service. The attack pattern is organized in such a way as to circumvent the methods proposed in the literature to detect attacks with low performance or for their significant delay. It does not display the periodic waveform typical of low bitrate exhaustive attacks. In contrast, it is an iterative and gradual process. In particular, the attack power (in terms of the speed of service requests and concurrent attack sources) is slowly increased by a patient attacker, resulting in significant financial losses, even if the attack pattern is based on the maximum size and arrival. work. The rate of service requests authorized in the system. Using an empirically developed simplified model, we derive an expression for a gradual increase in attack power depending on the achieved degradation of service quality (without prior knowledge of the target system power). We show that features offered by a cloud service provider to ensure a customer-agreed SLA (including load balancing and autoscaling mechanisms) can be maliciously exploited through a proposed stealth attack that slowly consumes the resources provided by the cloud. The supplier increases the costs borne by the customer. The proposed attack strategy, the Slow-Growing Polymorphic DDoS Attack Strategy (SIPDAS), can be applied to various types of attacks that exploit known application vulnerabilities to compromise a server-provided service. Targeted applications running in the cloud.

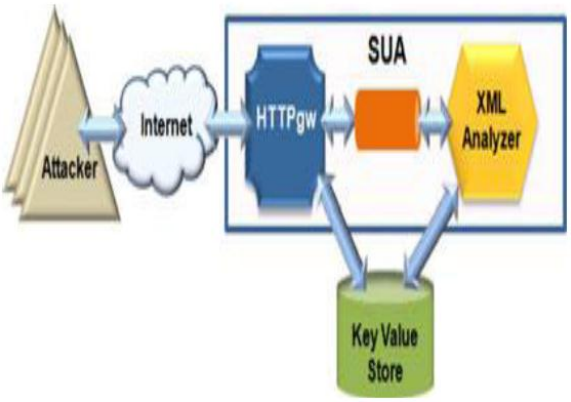


Fig. 1: Functional diagram of the proposed system.

5. DESCRIPTION OF MODULES

A. Server model under attack:

To assess the quality of service degradation associated with an attack, we define a synthetic representation of the attacked system. We assume that the system consists of a group of distributed virtual machines that are provided by a cloud provider and that run application instances. We also assume that there is a load balancing mechanism that distributes user service requests across instances. The number of instances can be automatically increased or decreased by

tracking certain relevant parameters to assess the quality of the services provided (for example, computational load, memory used, and number of active users). Specifically, we simulate an attacked system with total capacity, which is the total amount of work that the system can do to process service requests. This ability is influenced by various parameters, for example. For example, B. number of virtual machines assigned to the application, processing power, storage capacity, etc. Each service request consumes a certain capacity depending on the payload of the service request. Thus, the system load CN at time t can be modeled by a queue system with Poisson arrivals, exponentially distributed service time, multiple servers, and n current incoming requests (system throughput). In addition, cloud autoscaling is modeled in a simple way: when new resources (such as virtual machines) are added to the system, it increases the capacity of the system.

B. Creation of wear in service:

Imagine a cloud-based system with full service request processing capabilities and a B-size queue that represents a common bottleneck for client and DoS flows. Use C0 to indicate the load at the beginning of the attack period T (assuming this is at time t0), and CN as the load to process user requests on the target system during the time window T. destination, the number of threads n must be organized. ...

C. Minimize the visibility of attacks:

According to the previous definition of a covert attack, conditions must be met to reduce the signature of the attack. Hence, the patient and the experienced attacker should be able to detect the application of the vulnerability (for example, a deeply nested XML vulnerability) by scanning both the target system and legitimate service requests (for example, for HTTP messages, including the XML document structure).) and identify the set of types of legitimate service requests that could be exploited to exploit this vulnerability. For example, in an X-DoS attack, an attacker could implement a series of XML messages with a different number of nested tags. The NT threshold can be arbitrarily set, or possibly estimated during a training phase in which an attacker inserts a sequence of messages with an increasing number of nested XML tags to identify a possible threshold-based XML validation constraint. A similar approach can be used to estimate the maximum message rate at which service requests should be inserted.

D. XML-based DoS attack

In a pilot campaign, we analyzed CPU utilization based on the number of nested XML tags and the frequency with which malicious messages were injected. In particular, the CPU consumption on the target system for parsing messages containing XML tags with different nesting depths. [t] Results showed that messages from 500 nested beacons are enough to generate a maximum CPU utilization of about 97%, while with 1000 beacons the processor processes the entire message in about 3 seconds. In addition, we carry out various attacks. For each attack, we introduce a uniform XDoS stream, that is, a sequence of messages with a fixed number of nested tags and a fixed message rate. Let us assume that 20 seconds is the maximum experimentally observed time to reach the stable state value of the attacked processor (ie CR), and denote the "baseline" as the average processor load in the absence of user load (about 9%). There are several ways to implement a SIPDAS based attack. In this work, we use the same cloud framework that we used to create a targeted server application.

6.RESULTS

We demonstrate that the proposed slow-growing polymorphic behavior causes significant overload on the target system (resulting in significant financial losses) and significantly bypasses or delays detection methods. Even if the victim detects an attack, the attack process can be restarted by exploiting another application vulnerability (form polymorphism) or synchronization (time polymorphism) to increase the consumption of extended resources.

7. CONCLUSION

In this article, we propose a strategy for implementing stealth attack schemes that exhibit slowly growing polymorphic behavior that can significantly evade or delay methods proposed in the literature for detecting underperforming attacks. By exploiting a vulnerability in the target application, a patient and a smart attacker can coordinate complex message flows that can be distinguished from legitimate service requests. Specifically, the proposed attack model seeks to take advantage of the flexibility of the cloud, rather than making the service unavailable and forcing the services to scale and consume more resources than necessary, making the cloud client more financial than when it comes to a service issue availability.

REFERENCES

1. H. Sun, J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proc. 12th IEEE Int. Conf. Netw. Protocol., 2004, pp. 196-205.
2. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.
3. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.
4. M. Ficco, "Security event correlation approach for cloud computing," Int. J. High Perform. Comput. Netw., vol. 7, no. 3, pp. 173–185, 2013.
5. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.
6. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

USING MEAN OPINION SCORE FOR QUALITY ANALYSIS OF MPEG-4 VIDEO IN NS-2

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

1Professor, 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, (15RG1A04C9, 15RG1A04D0, 15RG1A04D1, 15RG1A04D2), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Recently, many telecommunication systems apparently support various types of real-time transmission, and video transmission is one of the most important applications. Studies today show that around 60% of the data on social networks and other internet applications uses streaming video. Therefore, the increasing demands of telecommunications operators require sophisticated methods and procedures to provide high quality, real-time video transmission in a limited bandwidth paradigm. Some scientists have slightly improved the video streaming properties such as packet loss rate, packet delay or packet jitter. However, the above quality settings cannot be easily and clearly converted into a high quality video stream. The disadvantage of these parameters is that their transformations are different for each coding scheme, each loss obfuscation and each jitter management. Commercially available tools for assessing video quality often require synchronized frames on both the sending and receiving sides. However, this supposed frame synchronization cannot be applied if frame drop and frame decoding errors occur. JNDmetrix -IQ and AQUAVIT software are the tools that are available to the public in today's market, but they cannot evaluate incomplete received videos on the receiving end. These apply to the video frame, which can be decoded on the receiving end without jitter or loss of delay in this role

Keywords— MPEG, NS-2, ad hoc networks, PSNR, MOS.

1. INTRODUCTION

The maximum signal-to-noise ratio, abbreviated as PSNR, is a technical term for the fraction between the highest possible power of a signal and the power to distort noise, which affects the reliability of its representation. Because different signals have an incredibly large dynamic range, PSNR is usually pronounced in logarithmic decibel scale arrangements for measurement. PSNR is typically used to determine the recovery quality of the lossy compression codec (e.g. for image compression).

PSNR is mainly defined by the root mean square error, also known as MSE.

In a silent m × n monochrome image I and its noisy approximation K, the MSE is defined as:

PSNR (in dB) is defined as:

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left[I(i,j) - I'(i,j)\right]^2$$

Typical PSNR values for lossy video and image compression are between 30 and 50 dB as long as the bit depth is 8 bits, which should always be higher. For 16-bit data, typical PSNR values are between 60 and 80 dB. Acceptable values for the loss of quality in wireless communication are between 20 dB and 25 dB.

The PSNR block calculates the maximum signal-to-noise ratio (PSNR) in decibels between two images. This ratio is usually used as a quality quantity between the original image signal and a compressed image signal. The higher the PSNR of a picture signal, the better the quality of the compressed or reconstructed picture signal.

There are two types of error metrics used for image compression quality. One is known as the root mean square error (MSE) and the other is known as the peak signal-to-noise ratio (PSNR). To calculate the PSNR, the header mainly calculates the root mean square error using the following equation:

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left[I(i,j) - I'(i,j)\right]^2$$

MSE and PSNR are the algorithms used in image processing to evaluate the performance of the codec of interest. They are closely related to each other and borrowed from other signal processing contexts. PSNR is one of the most commonly used objective measures to assess the quality of service of video streams at the application level. The following equation shows the definition of the PSNR between the luminance component Y of the source image S and the destination image D:

PSNR (n) dB = 20

$$\left(\frac{V_{peak}}{\sqrt{\frac{1}{N_{col}N_{row}} \sum_{i=0}^{N_{col}N_{row}} \sum_{j=0} [Y_S(n,i,j) - Y_D(n,i,j)]^2}} \right)$$

where Vpeak = 2k-1 and k = number of bits per pixel, also known as the luminance component. PSNR calculates the error between a reconstructed image signal and the original image signal. Before transmission, a sequence of reference PSNR values can be calculated when reconstructing the encoded video against the original raw video. After transmission, the PSNR is calculated at the receiver for the video that has been reconstructed from the possibly corrupted received video stream.

2 Effects of bandwidth, block size and CER on the PSNR

The maximum signal-to-noise ratio in multimedia traffic is examined by varying the parameters. First we varied the block size and the channel error rate (CER) for different sets of bandwidth and measured the PSNR. The following results are observed.

The results are broken down according to bandwidth

2.1 PSNR with a bandwidth of 0.5 Mbit / s

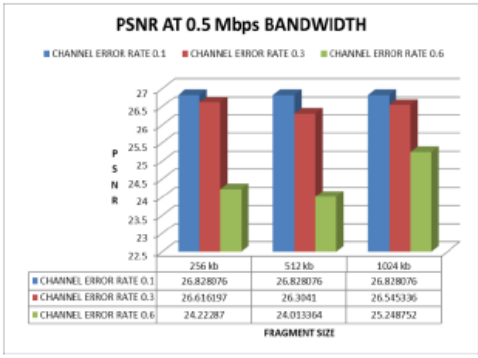


Figure 1.1: Graphic for PSNR at 0.5 Mbit / s

In the above output, the bandwidth is set to 0.5Mbps, the size is increased from 256KB to 1024KB, and the channel error is slightly changed from 0.1 to 0.6, then the peak ratio signal. The noise improves from 26.828076 initially to 24.22287 at 256 kb then from 26.828076 to 25.248752 at 1024 kb. For example, in CER 0.6 the size is 256 kb and the PSNR is 24.22287, and it improves to 25.248752 when the size is increased to 1024 kb.

2.2 PSNR at 1.0 Mbit / s bandwidth

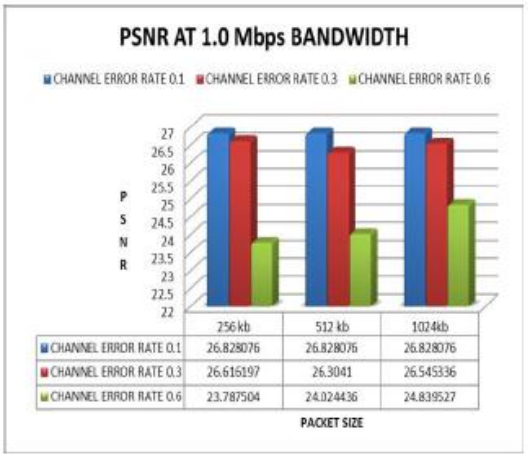


Figure 1.2: PSNR diagram with 1.0 Mbit / s

The graphic above shows the PSNR at 1.0 Mbit / s with the channel error rate fixed and the block size increasing. This graph suggests that the maximum signal-to-noise ratio (PSNR) with variable channel error rate (CER) and fragment size over three sets of bandwidth shows that the PSNR improves for a higher error rate channel (CER) with a larger fragment. Cut.

2.3PSNR 2.0 Mbit / s bandwidth

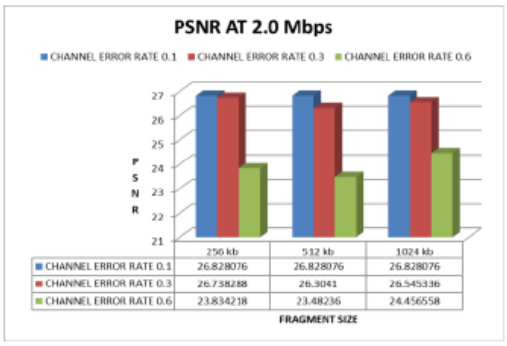


Figure 1.3: Graphics for PSNR with 2.0 Mbit / s

Analysis of the peak signal-to-noise ratio (PSNR) with variable channel error rate (CER) and fragment size in three sets of bandwidth shows that the PSNR improves for a higher channel error rate (CER) with larger segment size.

3 RESULTS

The results are created taking into account different results of the MPEG video peak signal-to-noise ratio (PSNR) in different settings and considered separately. However, the final conclusion is drawn by comparing the results. The individual PSNR values at the end of the source or the receiver don't mean much, but the difference between the quality of the video signal encoded at the source and the received video signal can be used as an objective QoS metric to study the impact of streaming on video quality. at the application level.

4 CONCLUSION

This article changes various parameters to increase the peak signal-to-noise ratio, since the peak signal-to-noise ratio is the ratio between the maximum possible power of a signal and the power to corrupt the noise that affects the fidelity of its sound in image compression. To improve the peak signal-to-noise ratio (PSNR), three parameters were changed, namely the channel error rate (CER) and the size and bandwidth of the data. Results shown in the figures above.

REFRENCES

1. Marc Greis' Tutorial for the UCP/LBNL/VINT Network Simulator "ns".
2. Teerawat Issariyakul and Ekram Hossain. "Introduction to Network Simulator NS2", 2nd ed. New York, Springer. 2012.
3. Emilio Raggi, Keir Thomas,Trevor Parsons, Andy Channelle, and Sander van Vugt. "Beginning Ubuntu Linux", 5th ed. New York, springer. 2010.
4. Raffaele Bruno, Marco Conti, and Enrico Gregori (2008), "Throughput Analysis and Measurements in IEEE 802.11 WLANs with TCP and UDP Traffic Flows", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 2, pp. 1233-1536.
5. Forouzan,. "Data communications and networking". 4th ed. New York, Tata McGraw-Hill publishing company limited. 2007.
6. IEEE computer society. "802 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture". New York. IEEE. 2001
7. Gilberto Flores Lucio, Marcos Paredes Farrera, Emmanuel Jammeh, Martin Fleury, Martin J. Reed, Mohammed Ghanbari and Fellow IEEE (2006), "Análisis a Nivel-Paquete de Simuladores de Red Contemporáneos", IEEE LATIN AMERICA TRANSACTIONS, VOL. 4, NO.4, pp. 299-307.
8. Christhu raj M.R, Namrata marium Chacko, John major and Shibin. D (2013), "A Comprehensive Overview on Different Network Simulators", International Journal of Engineering and Technology (IJET), VOL. 5, No.1, pp. 0975-4024.
9. S. Giannoulis, C. Antonopoulos, E. Topalis, A. Athanasopoulos, A. Prayati and S. Koubias (2006), "TCP vs. UDP Performance Evaluation for CBR Traffic On Wireless Multihop Networks", 5th International Symposium on Communication Systems, Networks and Digital Signal Processing, pp 154-158.

SECURED MESSAGES TRANSMISSION OF IN VEHICULAR AD HOC NETWORKS USING CONGESTION CONTROL TECHNIQUE

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

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS,
✉ narmadakari@mrcew.ac.in

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— The Vehicle Ad Hoc Network (VANET) is similar to MANET. Since there are mobile nodes in MANET, there are vehicles in VANET. If we compare it to MANET, VANET has different properties. When the channels are saturated with nodes, the channel becomes overloaded. The possibilities of network congestion increase as the number of collisions increases, and all of this is due to the increase in vehicle density. In this thesis we propose the RT-MMF algorithm to control the congestion in VANET and to transmit security messages through nodes using encryption and decryption techniques. We will also learn the performance of the proposed algorithm. We evaluate the result of our proposed method by simulating with NS2. In this article we also compare the state of the art with our proposed method.

Keywords— VANET, MANET, congestion control, RT-MMF, network simulator.

1. INTRODUCTION

Vehicle ad hoc networks (VANETs) use intelligent transport systems (ITS) to operate wireless communication in vehicle environments. VANETs provide users with a unified and safe environment to reduce traffic accidents, traffic congestion and fuel consumption, etc. VANet users can be informed of dangerous situations through vehicle communication and the exchange of information about the surroundings. To avoid this problem, warning messages should be sent to vehicles to avoid further collisions. We need to examine the likelihood of vehicles being sent and the safety messages received, as well as the delay that will occur in sending the message to the future recipient.DSRC [3] will not work properly in a high mobility environment.

2. LITERATURE REVIEW

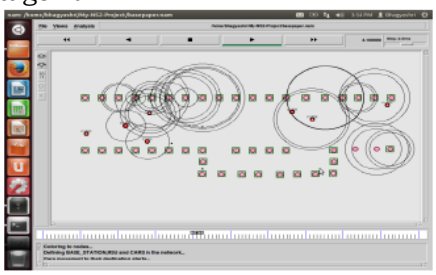
Varsha H ,, Pradeep, (IJCSIT) International Journal for Computer and Information Technology, Vol. 5 (2), 2014, [1] This document describes the performance evaluations of the transmission of safety messages in VANET in vehicle-to-vehicle communication (V2V) taken into account. Vehicles, which are viewed as nodes in VANET, communicate or exchange messages with one another, which is referred to as V2V or Inter-Vehicle Communication (IVC). V2V communication is implemented via the Dedicated Short Range Communication Protocol (DSRC) [3].

Meenal Pannase January 2014 [2] In this article we propose a priority-based congestion control algorithm to avoid congestion in the natural environment of the VANET. We are also investigating the production of a priority-based congestion control algorithm that has been proposed for VANET in various congestion scenarios.

4.ADAPTATION AND MOBILITY-BASED ALGORITHM (AMBA)

We are essentially comparing the system with two methods, one is AMBA, which has been used previously, and the other is our proposed RT-MMF system. So we will first see how the AMBA technique works. In principle, the Mobility Based Adaptive Algorithm (AMBA) enables more vehicles to send their status reports within the network.

Screenshot 1: Network structure in the AMBA algorithm



Screenshot 2 - Transmission of messages over the network

Screenshot 3 - A collision occurred while transmitting messages

However, a collision can occur while the messages are being transmitted between vehicles, as shown in Figure 3, and there may be a delay, but the packets lost during transmission by the nodes are high. The efficiency of this method is therefore low and the security provided for the transmission cannot be achieved either.

3.MAX-MIN THEORETICAL RELAXATION ALGORITHM (RT-MMF)

The design of our system can be divided into two main parts, namely Relaxation Theory (RT) and Max-Min Equity (MMF) [4]. The conceptual view of the original RT and the design flow diagram of our proposed system are shown in Figure 1. The two proposed methods are chosen because of their unique characteristics when dealing with congested networks.

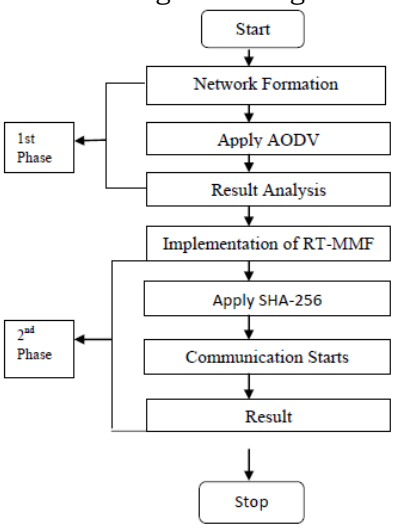


Fig. 1: Relaxation theory (RT) and Max-Min-Equity (MMF)

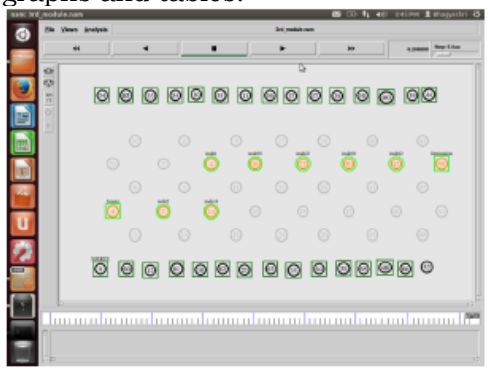
The system is divided into three modules. The first just shows the concept of active and deactivated network, the second is RT-MMF, which we saw in the flowchart in the previous figure: 1 and the third is the encryption and decryption algorithm. In the first module we showed how we can use the concept of active shutdown to save system energy. Because not all nodes participate in the transmission. In the second module we apply the RT-MMF congestion control algorithm. To control the overload, we apply the RT-MMF alWith this algorithm, EL is the most important factor if it exceeds the bandwidth threshold. Our communications will stop and EL will reset the algorithm we are using start using used is as follows.

Initialize EL = 0.
For (I = 0; I <length; I ++)
{
Repeat the communication from the source to the destination for the duration of the loop.
EI ++;
Yes (El == 250)
{
Break;}}
}}
Print ("The bandwidth limit exceeds the EI result at zero (0)");

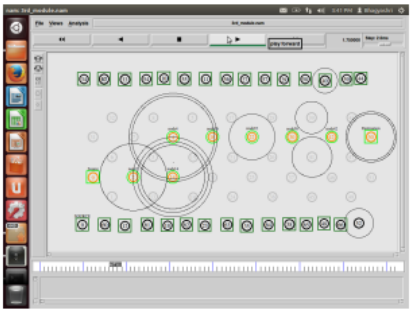
For security reasons, we use an encryption and decryption algorithm. In order to securely transfer messages from source to destination, we need to encrypt the message. We use the SHA-256 algorithm for this.

5. Results and discussions

The simulation [9] was approved using a powerful network simulator-2 (NS-2) [7] to determine the performance of the proposed method. RT-MMF was deliberately developed to provide a high traffic throughput with simultaneous data transmission in the WBSN [5]. In this section we first see our proposed system, then we see the comparison between the previous system and the one proposed by graphs and tables.



Screenshot 4: Basic view of the proposed system



Screenshot 5 - Packages being delivered from origin to destination

In screenshot 5 above we can see the packages being delivered from the origin to the destination. Since we use the actively deactivated concept, the packets only pass through the active nodes and thus we can save the energy and time that are required for the delivered packets.

6. CONCLUSION

In this project we discuss how the problem of traffic jams and collisions can be avoided. For evaluation purposes, we performed what-if analysis on NS-2 [12] and showed that RT-MMF still performed much better than the previous one in multi-node scenarios. Here we compare the results of two techniques, one of which was previously invented as AMBA and the other is the proposed RT-MMF technique. By using RT-MMF, overloads and collisions in the network can be avoided. RT-MMF can reduce congestion while transmitting data, which is an essential indicator of its efficiency. By using encryption and decryption, we can ensure the security of messages that are transmitted over the network. The energy required for execution takes less. If we calculate throughput, the ratio of packets delivered from origin to destination is greater than AMBA. From the results we conclude that our proposed system is more efficient than the previous one.

REFERENCES

Naimah Yaakob, Member, IEEE, and Ibrahim Khalil, Senior Member, IEEE," A Novel Congestion Avoidance Technique for Simultaneous Real-Time Medical Data Transmission", JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. XX, NO. X, FEBRUARY 2015.

Naimah Yaakob, Member, IEEE, and Ibrahim Khalil, Senior Member, IEEE," A Novel Congestion Avoidance Technique for Simultaneous Real-Time Medical Data Transmission", JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. XX, NO. X, FEBRUARY 2015.

Varsha H , Pradeep. S," Enhanced Performance Evaluation for Broadcasting Safety Messages In VANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1595-1598

Meenal Pannase Priority Based Congestion Control for VANET: Review International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 1, January 2014.

C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "(CODA): congestion detection and avoidance in sensor etworks," in Proceedings of the 1st international conference on Embedded networked sensor systems, ser. SenSys '03. New York, NY, USA: ACM, 2003, pp. 266–279.

N. Yaakob, I. Khalil, and J. Hu, "On the effectiveness of relaxation theory for controlling high traffic volumes in body sensor networks," in Proceedings of the 2nd International ICST Conference on Wireless Mobile Communication and Healthcare Mobihealth. Greece: Springer, 2011, pp. 16–23.

ARTIFICIAL INTELLIGENCE FOR VEHICLE DETECTION AND SELF DRIVING USING FUZZY CLUSTERING ALGORITHM

Venkatesham Veerannapeta[1]., K.Jahnavi 2., K.Krishnapriya 3., K.Pushpa4., K.Vasavi5.,

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

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0459, 15RG1A0445, 15RG1A0429, 15RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: ***This article describes how to track and detect unmanned vehicles using the FCM algorithm. To achieve this, artificial intelligence is used to identify and track a path that a smart car can follow. The disadvantage of using the ray model based algorithm is that they cannot detect and track dynamic vehicles that are obscured by other objects and cannot move in the right direction when an obstacle occurs in the center. To solve this problem, a new ALV detection and monitoring algorithm is proposed. Scaling up the frame rate increases the temporal sampling rate in progressive video.***

Keywords: unmanned ground vehicle (ALV), vehicle detection and tracking, artificial intelligence, fuzzy clustering algorithm, Hough transformation

1 Introduction

Over the past hundred years, advances in the automotive industry have made vehicles safer, cleaner, and more affordable, but the advances have been gradual. The activity now appears to be approaching a significant change brought about by autonomous or unmanned driving. The term “unmanned car ” was characterized as follows. A car that can drive freely without human control. In many cases, the vehicle customer can physically activate or deactivate this component . This innovation offers the possibility of remarkable benefits for a life that preserves social well-being. Reduce accidents, clogging, fuel consumption and pollution; Expanding versatility for people with disabilities; and finally improve land use.

2. Related work

Simultaneous localization, mapping and tracking of moving objects (SLAMMOT) includes both the simultaneous localization and mapping (SLAM) in dynamic environments as well as the detection and tracking of these dynamic objects. A math framework will be established to incorporate SLAM and tracking of moving objects. Simultaneous localization and mapping (SLAM) as well as detection and tracking of moving objects (DTMO) play a key role in robotics and automation [1]. The pattern classification strategy and the pixel-based change detection technique are used. The sparse generative model (SGM) is used to track different objects at different speeds and shapes [2]. Bayesian Occupancy Filter (BOF) system to shorten the set-up time and improve the consequences for the resulting cluster and the subsequent calculation in the light of BOF [3]. A modified SMC-BOF demarcation technique anticipates habitability frameworks. The first SMC-BOF was generally used in the context of mapping the habitability network because it reduced computational costs compared to the BOF technique [4]. Mapping the state of the habitability framework is a key process for mechanical autonomy and autonomous driving frames. Divide the earth into network cells with data states. A modified SMC-BOF technique to delimit the expected habitability framework. The first SMC-BOF was generally used in the context of grid mapping because it has lower computational costs than the BOF technique.

3. PROPOSED WORK

In the proposed work, the drone is to take a correct path when an obstacle is made there by calculating the distance from the right and left directions in the shape of a column. The video is converted to an image and the functionality is extracted using the Hough transform and the decision is made.

3.1. Capture video through the image pipeline system

When capturing video with the Frame Pipeline framework, upconverting the edge speed increases the speed of cursory inspection in dynamic video. On-board speed transformation boxes integrate the passage of a digitized movie that was shot at a banal speed of 24 fps. With the NTSC layout, which requires 60 fields / s. The result is a video recording using the Frame Pipeline framework. Increasing the edge rate increases the overall test rate in dynamic videos. Edge Speed Transform Boxes contain

digitized film changes that were recorded with a transition speed of 24 edges / s. For the NTSC design, which requires 60 fields / s. The result is a clearer picture, especially in the middle of a moderate motion video.

3.2. Segmentation of road objects by maximizing pixel expectation of movement (MPEM)

Maximizing the pixel expectation of Road Object Division (MPEM) motion is achieved by applying the desired magnification calculation. Motion estimation is the way to compute motion vectors by finding coordinated parts further along the edge to compare them to obstacles on the current edge. Estimating the movement makes it possible to see the temporary surpluses. Various tracking calculations were performed to evaluate the movement. The basic suspicion behind these calculations is that the exclusive translational motion can be compensated for by rotational motion and the zoom cannot be evaluated using quadratic tracking calculations. It is known to be the most important and computationally focused process in computing video pressure.

3.3. Hough transforms feature extraction for track recognition

Highlighting the Extraction: The second requirement includes the Hough Transform Extraction of the preparatory organization. Each annotated part is scaled and rotated to an authorized position that precedes learning. The preparation kit contains small changes to the scale, rotation and counterweight in the first photos. The negative element vectors are obtained by constantly examining them from areas of the image outside of the skipped question field. After the preparation of the underlying classifiers, false positive results are again increasingly generated by the underlying classifier with a different set of negative preparations. The second order transformation is calculated as autocorrelation, contrast, correlation, cluster prominence, cluster shadow, dissimilarity vitality, entropy, homogeneity, maximum probability, sum of squares, normal sum, fluctuation, entropy sum, change in difference, difference entropy.

3.4. Searching and recognizing poses using the deep web with track space estimation

Posture search and detection of a deep autonomous driverless steering system with path space using evaluate the base contour by taking the normal of the considerable number of pixels. The number of the plan was selected from which the follow-up to a complaint should begin. Chosen from the Edition Framework episode, it was chosen by repositioning the veil. For the selected question, its position of the center of gravity and the whole time and the estimation condition were determined from the center of gravity data.

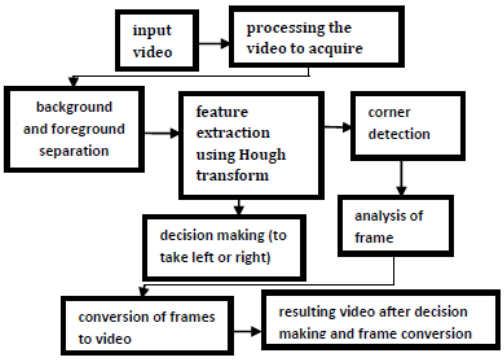


Figure 3.1 Function diagram

4. TEST RESULTS

MPEM enables automatic detection of objects and movement without a grid. The extraction of second order features is performed using the Hough transform. Deep Web Pose Search and Recognition with Track Space Estimation is performed to provide a spontaneous result.

Figure 4.1 - Capture the input video

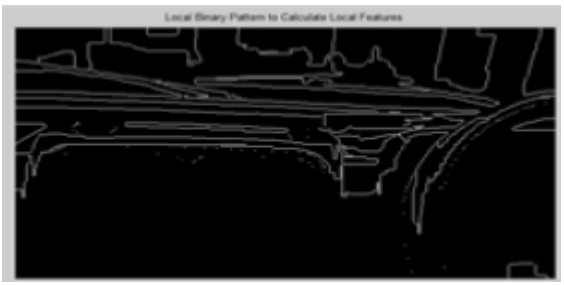


Figure 4.2 - Conversion to a binary pattern for calculating the local characteristic

Figure 4.3 - Detection of an existing obstacle

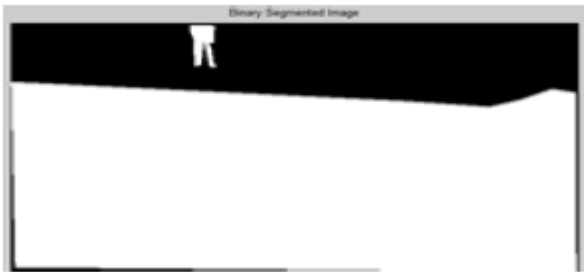


Figure 4.4 - Binary segmented image

Figure 4.5 - Lane Detection When Turning Left or Right

Figure 4.6 - Converting the processed image to the final video

5. CONCLUSION

A vehicle measurement model based on probability fields combined with our newly modified FCM video segmentation algorithm and Hough's transform characteristic extraction is proposed to estimate the poses of vehicles in which you can naturally drive the situation where dynamic vehicles are completely different from others Objects are covered in the xy plane.

References

1. J. Leonard et al., “A perception-driven unmaned urban vehicle,”mhJ. Field Robot., vol. 25, no. 10, pp. 727–774, Oct. 2008.
2. Y. Yang, G. Yan, H. Zhu, M. Y. Fu, and M. L. Wang, “Moving object detection under dynamic background in 3D range data,” in Proc. IEEE IV Symp., 2014, pp. 394–399.
3. M. Himmelsbach and H. J. Wuensche,”Tracking and classification of ar-bitrary objects with bottom-up/top-down detection,” in Proc. IEEE Intell.Veh. Symp., 2012, pp. 577–582.
4. D. Z. Wang, I. Posner, and P. Newman, “Model-free detection and tracking of dynamic objects with 2D lidar,” Int. J. Robot. Res., vol. 34, no. 7,pp. 1039–1063, Jun. 2015.
5. T. Gindele, S. Brechtel, J. Schroder, and R. Dillmann, “Bayesian occupancy grid filter for dynamic environments using prior map knowledge”in Proc. IEEE IV Symp., 2009, pp. 669–676.
6. R. Danescu, F. Oniga, and S. Nedevschi, “Modeling and tracking the driving environment with a particle based occupancy grid,” IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 1331–1342, Dec. 2011.

LICENSE PLATE RECOGNITION USING LAPLACIAN EDGE DETECTOR AND FEATURE EXTRACTION FOR INTELLIGENT TRANSPORT SYSTEMS

Boini Nareshkumar[1]., K.Jahnavi 2., K.Krishnapriya 3., K.Pushpa4., K.Vasavi5.,

1 Associate Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, ✉ nareshboini@gmail.com

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0459, 15RG1A0445, 15RG1A0429, 15RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: License plate recognition is an important research area for several reasons. When it comes to recognizing the number of a moving vehicle, it has its own challenges that need to be addressed. In this work a real-time system was proposed to locate and identify the license plate of moving vehicles. First, the Otsu method is used to treat the noise in the captured image of the vehicle. The image is then binarized and the license plate is located using the Laplace operator. In addition, the characters on the disk are segmented and normalized. Finally, the characters on the disk are recognized using the feature extraction technique. The proposed system has the ability to extract the characters under different environmental conditions. It can also detect bad characters in the license plate and characters that are written in multiple strokes. The experimental results applied in the proposed system promise a high efficiency rate. The end of this document suggests some future advances in the license plate recognition system.

Keywords: binarization, Laplace operator, feature extraction, segmentation, normalization

1 INTRODUCTION

The number of vehicles on the roads is increasing day by day. This has led to the need and development of the latest technologies such as intelligent transport systems (ITS). A popular application of this technology is Vehicle License Plate Recognition (VLPRs). This system is widely used around the world to contain criminal activity. Other areas in which this system is used include parking lots, traffic management, which ensures compliance with traffic rules and regulations, and automating the manual comparison of vehicle license plates, which reduces human effort. An efficient VLPR system can be used to track vehicles in real time, which turns out to be a boon to the traffic management system.

2. LITERATURE REVIEW

In 2011, a new approach to "function-based license plate location" was used to detect license plates in a mass surveillance system [11]. The system focused on two algorithms, viz. Search and filter window edges. This approach was based on the concept of image processing convolution, in which a window with a size corresponding to the size of the license plate is scanned over the vehicle image in order to capture the actual position of the license plate. Characters are recognized on the disk by pattern matching, the standard characters are stored in the database and then compared with the characters on the disk. This approach was limited to analyzing the rear

In 2013 SG Patel proposed a VLPR system based on morphology and neural networks [6]. The Sobel operator was used to detect edges. Morphological operations such as erosion and dilation were then used to create a smoother binary image of the license plate. The characters extracted from the disk were recognized by analyzing the statistical properties of the characters using the neural network. The problems

3. PROPOSED SYSTEM

The VLPR system proposed in this document focuses on two important issues for which previously developed approaches have produced incorrect results. The first problem is managing the different sizes of Indian license plates. The second major challenge is to recognize the characters that are written in multiple scripts, which are mostly English and Hindi. The system is divided into two components, viz. VLPR online and VLPR offline. The inline module consists of a high resolution camera or other visual device that is mounted along the streets and is used to provide input images to the system. The other component takes over all the processing of the images received by the camera, locates the license plate and finally recognizes the characters on the plate in order to identify the vehicle. The full operation of the proposed system is described as a series of following steps.

3.1 Image acquisition

The images of vehicles traveling on the road are captured by digital cameras installed on the roadsides or with traffic signs. Thanks to advances in visual machines, it is possible to get high resolution images of vehicles moving at high speeds of up to 150 km / h. The cameras must also be activated using infrared technology to take pictures at night. The

following figure shows a test image of the proposed system.

3.2 Conversion of gray levels

The vehicle image received by the camera is in digital form as shown in Figure 1. This is a full color RGB image that is converted to a grayscale image before processing. In the proposed system we used the brightness method to get the grayscale image. The intensity of each pixel is calculated by the following equation.

Grayscale image = (0.33 * R) + (0.59 * G) + (0.11 * B)

The converted grayscale image is shown in Figure 2 (b).

Fig. 1: Input image in RGB form

3.3 Image binarization

The grayscale image is now binarized, i.e. H. converted to a black and white image. Otsu's Threshold Method is used to do this process where we choose a threshold to differentiate the colors in the image. Values below the threshold are given a black color; H. 0 and the rest is assigned the color white, ie. 1.

This method is mainly used because of its accuracy in calculating the threshold and the low calculation cost. The resulting image is shown in Figure 2.

Fig. 2: Binarized image using the Otsu method

3.4 Elimination of image noise

The purpose of removing noise (unwanted information) from the image is to reduce the overhead of the noise sensitive edge detection operator. The median filter is used to remove image noise. There are other filters that can be used as well. However, the benefit of using a media filter is that it doesn't blur the edges of the image.

3.5 Position of the license plates

This is the most important step in the VLPR system and determines the overall success of the discovery process. In this approach, we used the Laplace operator to see the edges of the image first. The Laplace operator works on the convolution principle and, in contrast to other edge detectors such as Sobel or Prewitt, uses a second order derivation mask. Therefore, the Laplace operator can detect vertical and horizontal edges at the same time, as shown in Figure 3.

After applying the edge detection, an edge scanning operation was performed on the image to detect the exact position of the license plate as shown in FIG. The area of the plate in an image is typically a high intensity area that can be defined by contours that have similar properties.

Fig. 3: Localized license plate

3.6 Segmentation and normalization of characters

After the license plate is placed over an image, the license plate characters are segmented using the row-column scanning method shown in Figure 4. In this approach, we first scan the license plate horizontally to find the height of the characters and then vertically to calculate the width of each character.

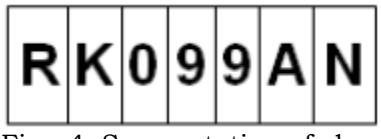


Fig - 4: Segmentation of characters

3.7 Character recognition

Instead of storing the patterns for each character, we trained the system to extract the raster properties of each character regardless of the English or Hindi script. Each character is divided into a grid and the number of black pixels in each part is calculated. For example, if two characters have the same properties. In

B and 8, the internal structural analysis is performed using the string coding technique for greater precision.

4. EXPERIENCE AND RESULTS

The license plate recognition system proposed in this document was successfully developed in Java and tested on an Intel Core i5 system with 4 GB of RAM. A database has been created in which the images received by the camera and the license plates recognized are saved. The output of the system was displayed to the user as a text file. The images captured as input were captured under various environmental conditions such as day, night, shadow on the plate, and so on.

Table 1: Comparison of the different approaches to license plate recognition

Approach	Merit	Demerit
Morphological Operations [6]	Easier to implement	High computation costs due to statistical features
Sliding Concentric Window [11]	Efficient in bright and illuminated images	Must adapt to the varying sizes of the license plates
Localization based on color information [8] [14]	Ability to detect deformations in the license plate	Not suitable during night hours

In the data set of 150 images, the proposed system successfully recognized 144 images with an accuracy of up to 96%. In some images in which more than one vehicle passed the camera, the system successfully recognized several license plates, provided they were not covered by another vehicle or object. The comparison of the proposed system with other approaches in the field of license plate recognition is shown in Table 1.

5. CONCLUSION AND FUTURE WORK

This article introduces a quick and efficient approach to license plate recognition based on edge detection using a Laplace operator which, when combined with contour analysis, can identify multiple license plates in one image. Another major problem solved by this system is the detection of disks on which characters have been written in various scripts. The execution method based on string coding is used for this. The system thus solves the two main problems that Indian license plates encounter. Apart from that, this article also introduces an approach to dealing with blurry images of vehicles using morphological techniques.

The method proposed in this article works in real time and can be used in various applications such as parking systems, automatic toll collection, traffic management, criminal activity reduction, etc.

Future advances in license plate recognition may include the use of better optical technologies to capture more precise images of vehicles moving at very high speeds. The location and segmentation of the plaque region against a complex background continues to challenge VLPR systems around the world and further studies in this area are needed.

REFERENCES

Singhadia and B. Patel, " Review on Automatic Number Plate Recognition System Using Improved Segmentation Method ", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, pp. 752 - 756, September 2014.

S. G. Patel, " Vehicle License Plate Recognition using Morphology and Neural Network ", International Journal on Cybernetics and Informatics, Vol. 2 – No. 1, pp. 1 - 7, February 2013

B. Singh and V. H. Deepthi, " Survey on Vehicle Number Plate Localization ", International Journal of Computer Applications, Vol. 67 – No. 23, pp. 7 - 12, April 2013.

Puranic, Deepak K. T. and Umadevi V., " Vehicle Number Plate Recognition System: A Literature Review and Implementation using Template Matching ", International Journal of Computer Applications, Vol. 134 – No. 1, pp. 12 – 16, January 2016.

N. D. Swathi and T. Saikumar, " Localization of License Plate Number using Dynamic Image Processing Techniques and Genetic Algorithm", International Journal of Scientific Engineering and Technology Research, Vol. 04, pp. 5598 - 5604, August 2015.

Kumar and S. Godara, " A Review : On Number Plate Recognition ", International Journal of Science and Research, Vol. 4, pp. 1964 – 1967, May 2015.

Dr. Dharun V S and Reji P I, " License Plate Localization : A Review ", International Journal of Engineering Trends and Technology, Vol. 10 – No. 13, pp. 604 - 615, April 2014.

MFCC & SVM FEATURE MAPPING BASED SPEAKER RECOGNITION & IDENTIFICATION

Arakatla Mamatha[1]., K.Jahnavi 2., K.Krishnapriya 3., K.Pushpa4., K.Vasavi5.,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ mamatha.2087@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (15RG1A0459, 15RG1A0445, 15RG1A0429, 15RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract - Recognition of speakers is now a source for the development of security. Speaker recognition has a wide range of applications in future applications such as voice dialing, database access services, information services, security control, hospitals, laboratories, industries, etc. With speaker recognition, the speaking person is checked and automatically identified. This project makes it possible to recognize the person who is speaking. Speaker recognition consists of two main parts: speaker identification and verification. Speaker recognition can be performed using two methods, which are text dependent and text independent. This document represents the identification and verification of the speaker through a language-dependent process. In this process, the properties of the voice are first extracted and then these properties are compared or checked in order to identify the speaker. Here we use MFCC (Mel Frequency Cepstral Coefficient) for feature extraction because it offers excellent performance to make it robust, accurate, faster and computationally more efficient. SVM (Support Vector Machine) is also used for feature mapping.

Keywords: speaker recognition, speaker identification, speaker verification, text dependent, text independent, feature extraction, MFCC, SVM

1 INTRODUCTION

The most practical form of communication since ancient times has been to talk to one another, that is, to talk to one another. Whenever we talk to someone, we give them information in the form of words or voices or, to be sure, we make the speech because this project is related. When air passes through a person's vocal apparatus when they speak, breathe, etc., the vocal cords reflect that air, which in turn produces speech. Therefore, speech occurs due to vibration in the vocal system of a human body. Since everyone has a different vocal apparatus, they produce different noises or speeches. The aim of this project is to identify and thus verify different speeches or people. This recognition of a specific person by their speech using a biometric device is done automatically using MFCC and SVM. MFCC and SVM are used because they offer maximum precision compared to LPCC, LPC, HPC, etc. Human height (an important characteristic of the human voice) depends on the change in background noise (traffic, bird chasing, unwanted noises), human emotions (stress, happiness, envy) and human health problems (cough, cold). These deviations can easily be eliminated in MFCC and SVM and offer a high accuracy of up to 95%. They are also easy to use.

2 SPEECH PRODUCTION

Speech is generated with the vocal cords. A person's vocal system is responsible for producing speech. The human vocal system includes the nasal cavity, lips, teeth, glottis, tongue, roof of the mouth, larynx, etc.

Figure 1: Human speech production system

" Speech is created by atmospheric pressure waves emerging from a speaker's mouth and nostrils." What defined by Huang et al. (2001) [1]. In other words, language is the ability to express feelings and thoughts through flowing sounds and gestures.

2.1 Speech Recognition

Speech recognition is nothing more than the transmission of information to a computer so that it recognizes what we are saying and, ultimately, in real time.

Speech recognition has two functions for identification and verification. During language identification, the speaker is identified from the database. This is a 1: N match. The voice specified in the entry is compared with the voice available in the database until the voice matches. If the vote matches, it means that the vote in the database N is identified. Otherwise

the output is "Match not found". Verification of language is the process of accepting or denying a speaker's identity. This is a 1: 1 match. This is a linear process where the input voice is checked against a single date and the result is obtained as true or false, yes or no.

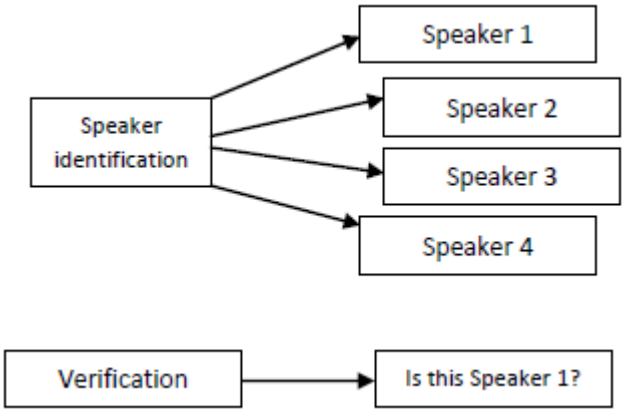


Figure 2: Speaker identification and verification process

Speech recognition can be performed through two processes:

Text-dependent: The text must be identical when adding (preparing the database) and when entering the entry for recognition. This is known as a text-dependent process. We can also use phrases or pins in this process.

Text independent: The process is called text independent if the text is different at the time of entry and verification. In this case there is no restriction on the text.

3. PROPERTIES OF EXTRACTION

This is the first and very important speaker recognition process. It extracts the main information from speech and removes other unnecessary data such as background noise and other interruptions (stress, emotions, environmental conditions).

3.1 MFCC

Mel's cepstral rate coefficient was introduced by Davis and Mermelstein in the 1980s. MFCC is the most popular and widely used technique in most speech signaling feature extraction applications [2]. We use MFCC because it is analogous to the human hearing mechanism.

The MFCC consists of five main stages: preprocessing, windowing, FFT (Fast Fourier Transform), mel-frequency envelope and cepstrum. The input signal is sent to the MFCC and we get the desired coefficient known as the MFCC.

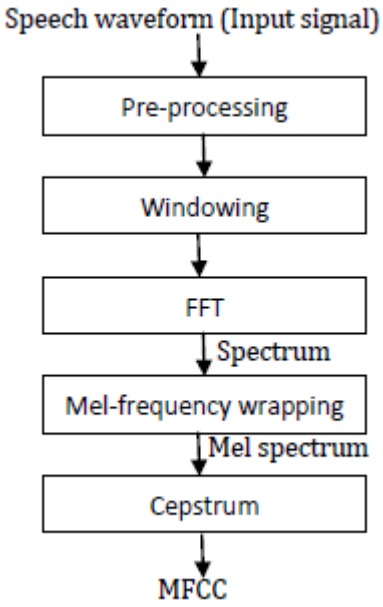


Figure 3: Extraction process of MFCC

Preprocessing: Preprocessing includes filtering. The filtering consists in converting the given speech signal into a form suitable for the computer. The preprocessing consists of separating the voice from the voiceless.

Window: Used to minimize spectral distortion. To do this, we use a Hamming window that is configured to perform frame alignment at 20-25 msec to achieve steady state behavior. The Hamming window provides continuity at the beginning and end of each image. Offers better frequency resolution. The result of creating windows is given as

$Y(n) = X(n) \times w(n)$

Where,

Y(n) – output signal

X(n) – input signal

w(n) – hamming window

FFT (Fast Fourier Transform): FFT is the most important step of MFCC and consists of making the Fast Fourier Transform of each frame that extracts the components of the signals at a rate of 10 ms. The fast Fourier transform converts every N number of samples from the time domain to the frequency domain. The FFT sizes are 512, 1024, 2048. They are used to achieve a frequency response of the size.

Mel frequency envelope: According to a psychological investigation, the human representation of the frequency content of voice or speech is not proportional or it can be said that it does not follow a linear scale. A mel scale is used to measure different tones. "A mel is defined as a thousand pitches of a 1 kHz tone [1]." The frequency of the Mel scale

can be approximated by the following equation:

$$B(f) = 2595 \log_{10}(1 + f / 700)$$

The spectrum simulation takes place via a filter bank. The triangular band pass frequency response is used as a filter bank. The position of the filter bank is also spaced using a Mel scale.

Cepstrum: The final stage of MFCC is cepstrum in this stage. The coefficients of the Mel spectrum are converted in the time domain using DCT (Discrete Cosine Transform). The result is obtained as an MFCC.

4. FEATURE MATCHING

Feature mapping identifies features from two similar databases. One is known as the source and the other is known as the destination.

4.1 SVM

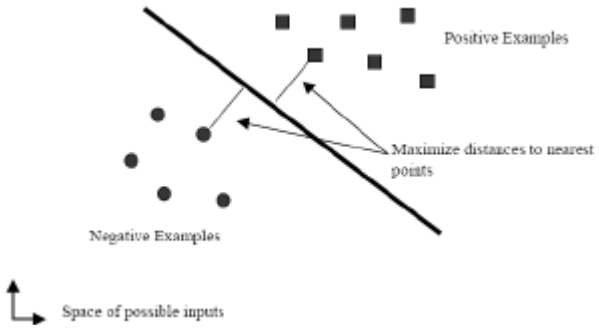


Figure 4: Linear Support Vector Machine

SVM is a simple and efficient algorithm. It is a linear classifier [4], ie it can only contain two components at a time and provides a proportional output. It can also be called a comparator as it has a binary output that translates to yes or no, accept or reject, 0 or 1, etc. In this project we are using more than two components for better efficiency, so we are using N SVMs.

5 RESULTS

This document describes a method for speaker recognition with MFCC and SVM. MFCC is used for feature extraction, while SVM is used for feature checking. The importance of MFCC and SVM and the reasons why they are widely used are adequately described in this document.

6. CONCLUSIONS

Using SVM techniques such as GMM (Gaussian Mixture Model) and HMM (Hidden Markov Model) can be used in the future as they are easier to use, require less data and offer greater accuracy. Future applications of this project are voice dialing on cell phones and telephones, hands-free calling via wireless Bluetooth headsets, biometric connection to telephone-based shopping systems and digital input modules.

REFERENCES

1. Geeta Nijhawan and M.K. Soni, “Speaker recognition using support vector machine”, International Journal of Computer Application, Volume 87-No.2, February 2014.
2. Huang, X, Acero, A. & Hon, H. “Spoken language processing – A guide to theory, algorithm, prentice hall PTR”, New Jersey (2001).
3. Jyoti B. Ramgire and Prof. Sumati M. Jagdale, “A survey on speaker recognition with various feature extraction and classification techniques”, IRJET, Volume 3, Issue 4, April 2016, pp. 709-712.
4. Simon Haykin, McMaster University, Hamilton, Ontario, Canada, Neural Networks a Comprehensive Foundation, 2nd edition, pp. 256-347.

ENERGY EFFICIENCY AND DATA TRANSMISSION ANALYSIS FOR UNDERWATER ACOUSTIC SENSOR NETWORK

Dr. K. Srinivasa Rao and Rajendra, E

1Professor, Department of ECE., TRR College of Engineering, Inole, Patancheru, TS, India,
(✉ drksrece@gmail.com)

1Professor, Department of ECE., TRR College of Engineering, Inole, Patancheru, TS, India

Abstract— Underwater Acoustic Sensor Arrays (UASN), which improve productivity and the unshakable quality of information transmission, are undergoing exceptional tests due to the complex underwater environment in various marine applications. The importance of using vitality in many UASN arrays using the productivity framework for 3D Squares View Vitality (EGRC) in UASN involves complex properties of the submerged average setting, e.g. B. scalable 3D topology, high proliferation delay, stroke and thickness portability and a group head ring rotation system. The events are controlled by the Trix perspective map and the 3D volume shape is divided into many small blocks in which a 3D square is viewed as a group. From the information transmitted with a specific end goal to make vitality productive and improve useful life, EGRC designs a demonstration of energy consumption taking into account the remaining vitality and surface area of the sensor concentrators to select the ideal group heads and then the base station . The waves generated by the submerged sensor concentrators provide an acoustic flag that selects the concentrator with the most noticeable excess vitality and the shortest distance from the base station as the main concentrator

Keywords— underwater acoustic sensor networks (UASN), energy efficiency and data transmission.

1. INTRODUCTION

Sensor centers at sea are considered to be applications conducive to oceanographic information collection, pollution monitoring, research at sea, fighting fiasco, assisted routes, and strategic intelligence applications. Numerous autonomous or unmanned underwater vehicles (UUV, AUV) equipped with submerged sensors will also discover application to the study of normal underwater resources and social events of logical information in community-based observation missions. In order for these applications to be suitable, it is necessary to improve the exchange of submerged equipment. Underwater vehicles and sensor centers must adapt themselves, meaning they must be able to organize their operations based on business design, territory and development data and transmit the observed information to an indoor station. Remote management of submerged acoustic systems is the innovation driving these applications. Acoustic underwater sensor networks (UW-ASN) consist of a variable number of sensors and vehicles that are sent to carry out collective observation missions in a specific area.

2. LITERATURE SURVEY

OssaiiiaYounis and Sonia Fahmy [1] proposed a new energy efficient approach to group nodes in ad hoc sensor networks. Based on energy-efficient distributed hybrid clusters, which cluster heads regularly select based on a hybrid from their residual energy and a secondary parameter, e.g. B. the proximity to their neighbors or the node quality. HuTian, Hong Shen, and Matthew Roughan [2] suggested how SNs can be placed using a minimum number to maximize coverage area when the communication radius of the SN is not less than the detection radius, resulting in results using one regular topology leads to WSN deployment. Rahimi, L. Shirachi [3] proposed the creation of a system called NIM where mobile collectors could only move along fixed cables between trees to ensure they could be recharged at any time while moving. Create a system called NIM where mobile collectors can only move along fixed cables between shafts to ensure they can be recharged anytime while moving.

3. EXISTING SYSTEM

This takes into account that the nodes of underwater sensors are connected to one or more underwater sinkholes by wireless acoustic connections. The data transmission takes place between the sensor nodes and the surface station through underwater sinkholes.

3.1 DISADVANTAGES

- The available bandwidth is limited.
- The propagation delay is very high.
- High bit error rate, temporary loss of connectivity can be investigated.
- The battery cannot be charged.
- Canal damaged by multiple ways and discoloration.

4. Proposed system

Underwater toilets are equipped with two acoustic transceivers, namely vertical and horizontal transceivers. Horizontal transceivers used by underwater wells to communicate with sensor nodes to send commands and

configuration data to sensors and to collect monitored data. Vertical link used by underwater wells to transmit data to the surface station. Vertical transceivers must be long range transceivers. Surface station with acoustic transceivers capable of handling multiple parallel communications with deployed acoustic submarine boreholes. It has been suggested that the basic cluster routing have a cluster header which is responsible for the path between the base stations and the node. Basic cluster routing is superior to multi-hop routing in terms of energy efficiency due to the lower data transfer. In basic cluster routing, each mobile node is divided into a network group with 2 hops in diameter. These disjoint sets or overlapping sets are defined as clusters. In each cluster, one node is selected as the cluster leader and another as a member node. The cluster head manages information in the cluster. The cluster-based routing protocol finds routes faster using flood minimization technology.

4.1 ADVANTAGES:

- The runtime delay is reduced.
- Connectivity and coverage problems are improved.
- The energy consumption is reduced.
- The node's fault is minor.
- The service life of the sensor is increased.

5. BLOCK DIAGRAM:

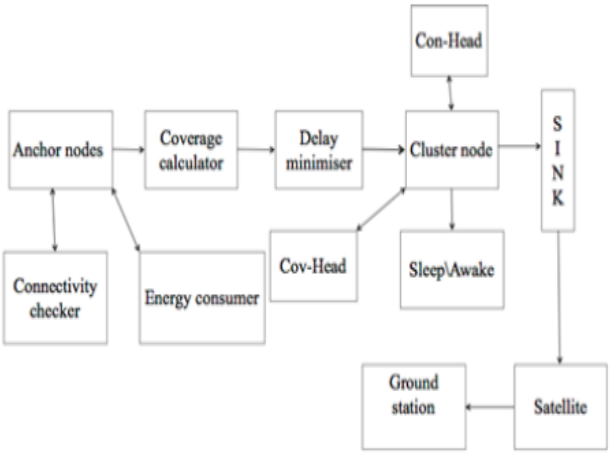


Fig. 1: Functional diagram of our proposed method

5.1 Communication model:

Creation of sensor nodes and borehole nodes. The nodes are placed within reach of the neighbor. When the sensor nodes want to transmit data, they send a request message to the neighbor. What is nearby sends a reply message to the node.

5.2 Cluster Head Formation:

Wireless communication and the lack of central administration pose many challenges for mobile ad hoc radio networks (MANETs). The mobility of nodes leads to frequent link failures and activations, causing the routing algorithm to react to changes in the topology and thereby increasing network control traffic. In the end, a CH can dominate so much MH that its computing, bandwidth and battery resources are quickly used up. The transmission period of the control messages must be adjusted dynamically in order to avoid unnecessary message exchanges when the node mobility pattern, e.g. B. a network topology is relatively static.

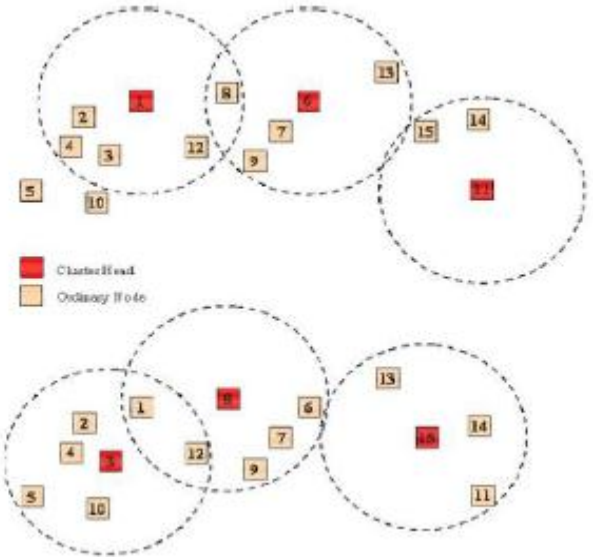


Fig 2: Cluster Head Formation

6. RESULTS AND DISCUSSION:

EGRC uses sustained vitality, zones and end-to-end transmissions to find the nearest jump center and maintain the unshakable quality of the information transmission. Recovery permits for the proposed computation are being made to demonstrate the adequacy of the EGRC, which outperforms agent computations in terms of vitality productivity, unshakable quality, and end-to-end delay. Finally getting better and better; Cluster Head manages data in the information cluster group and in the cluster system in order to avoid additional redundancies, improve the information inertia and optimize the use of the vitality of the entire system.

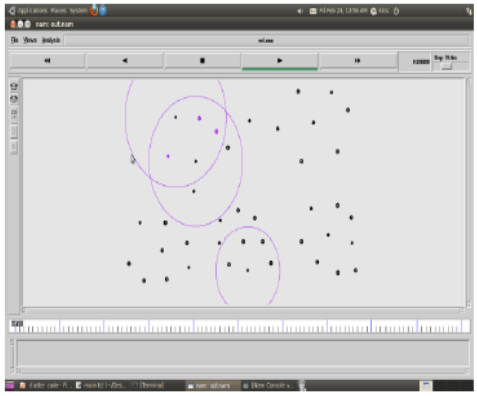


Fig 3 Sustained vitality in clusters

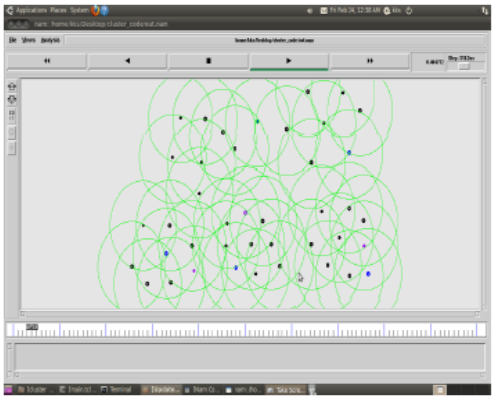


Fig 4 Clusters mapping

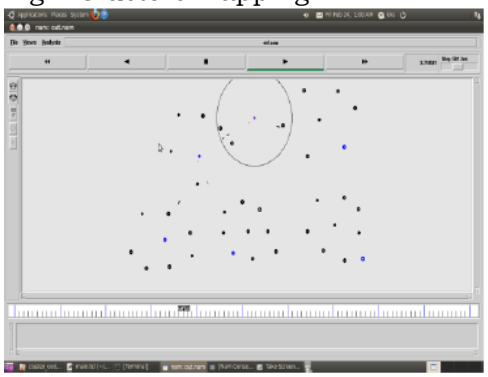


Fig5 Clusters Nodes Identification

CONCLUSION

Submerged applications have adhered to almost all lines of research. Has an understanding of the component of better alignment and better use of vitality. Problems that arise from my findings. Reflection and rationale behind the explanation of these disadvantages. Underwater applications have almost taken root in all areas of research. You have an idea of better energy use and routing mechanism. Problems that were formulated from my findings. Idea and logic behind solving these problems.

D. XML-based DoS attack

In a pilot campaign, we analyzed CPU utilization based on the number of nested XML tags and the frequency with which malicious messages were injected. In particular, the CPU consumption on the target system for parsing messages containing XML tags with different nesting depths. [t] Results showed that messages from 500 nested beacons are enough to generate a maximum CPU utilization of about 97%, while with 1000 beacons the processor processes the entire message in about 3 seconds. In addition, we carry out various attacks. For each attack, we introduce a uniform XDoS stream, that is, a sequence of messages with a fixed number of nested tags and a fixed message rate. Let us assume that 20 seconds is the maximum experimentally observed time to reach the stable state value of the attacked processor (ie CR), and denote the "baseline" as the average processor load in the absence of user load (about 9%). There are several ways to implement a SIPDAS based attack. In this work, we use the same cloud framework that we used to create a targeted server application.

6.RESULTS

We demonstrate that the proposed slow-growing polymorphic behavior causes significant overload on the target system (resulting in significant financial losses) and significantly bypasses or delays detection methods. Even if the victim detects an attack, the attack process can be restarted by exploiting another application vulnerability (form polymorphism) or synchronization (time polymorphism) to increase the consumption of extended resources.

7. CONCLUSION

In this article, we propose a strategy for implementing stealth attack schemes exhibit slowly growing polymorphic beha... that can significantly evade or delay methods proposed in the literature for detecting underperforming attacks. By exploiting a vulnerability in the target application, a patient and a smart attacker can coordinate complex message flows that can be distinguished from legitimate service requests. Specifically, the proposed attack model seeks to take advantage of the flexibility of the cloud, rather than making the service unavailable and forcing the services to scale and consume more resources than necessary, making the cloud client more financial than when it comes to a service issue availability.

REFERENCES

1. **H. Sun,** J. C. S. Lui, and D. K. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in Proc. 12th IEEE Int. Conf. Netw. Protocol., 2004, pp. 196-205.
2. Kuzmanovic and E. W. Knightly, "Low-rate TCP-Targeted denial of service attacks: The shrew vs. the mice and elephants," in Proc. Int. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2003, pp. 75–86.
3. M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.
4. M. Ficco, "Security event correlation approach for cloud computing," Int. J. High Perform. Comput. Netw., vol. 7, no. 3, pp. 173–185, 2013.
5. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.
6. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," Comput. Netw., vol. 51, no. 18, pp. 5036–5056, 2007.

USING LINK SIGNATURE IN WIRELESS NETWORK FOR IDENTITY BASED ATTACK DETECTION IN MIMO SYSTEM

Krishna Veni Adepu[1]., B.Lohitha [2]., B.Madhuri [3]., B.Lahari [4] B.Bavitha [5].,

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

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The signature of wireless connections is becoming increasingly important as wireless devices between a transmitter and a receiver to enable the authentication of wireless signals. This project identifies a new attack known as a mimicry attack against existing wireless signature schemes. It is assumed that an attacker "cannot" forge "any link signature" and that the attacker "does not have the same link signature on the recipient unless it is in the exact same location as the legitimate issuer ". The mimicry attack extends to MIMO systems (multiple input, multiple output). To defend against the mimicry attack, this project is based on the creation of a wireless connection signature, known as a time-synchronized connection signature, by incorporating the cryptographic protection and time factor into the properties of the wireless physical layer. This link signature is effective in authenticating the physical layer

Keywords— 1.MimoSystem, 2.Link signature, 3. Time synchronized

1. INTRODUCTION

The security of the wireless physical layer is becoming increasingly important as wireless devices become more ubiquitous and used in business-critical applications. In recent years, there have been several proposals to improve wireless security using physical layer functions including wireless device fingerprinting, wireless channel authentication and identification, and wireless channel identification. Deriving secret keys from channel properties. Recent advances in wireless physical layer security include link signing. The connection signature uses the unique properties of the wireless channel between a transmitter and a receiver to provide wireless channel authentication. There are three link signature schemes. The link signature was recognized as a physical layer authentication mechanism for applications where the wireless channel characteristics are unique to individual nodes.

2 LITERATURE SURVEY

Location differentiation is the ability to determine when a device has changed position. We are investigating whether it is desirable to use sophisticated PHY layer measurements in wireless network systems to differentiate location. We first compare two existing location discrimination methods, one based on the channel gains of multi-tone probes and the other based on the impulse response of the channel. We then combine the benefits of these two methods to develop a new measure of linkage that we call complex time signature. We used a 2.4 GHz link measurement data set obtained from CRAWDAD to evaluate the three location differentiation methods. We found that the complex time signature method works significantly better compared to existing methods. We are also doing new measurements to understand and model the temporal behavior of link signatures over time. We integrate our model into our location discrimination mechanism and drastically reduce the likelihood of false positives due to fluctuations in connection signatures over time.

3 EXISTING SYSTEM:

Existing techniques that use non-cryptographic approaches to authenticate wireless transmitters fall into three categories: Software

Fingerprint, location distinction and radiometric identification. RSS-based methods estimate the location of the origin of a signal directly on the basis of RSS values. However, these methods can be defeated with an antenna array that can spoof any source location. Approaches based on link signature authenticate the properties of the channel between sender and recipient. Radiometric identification approaches use the distinguishing features of the physical layer presented by wireless devices to distinguish them.

3.1 DISADVANTAGES:

• Existing signature schemes for wireless connections are not suitable for mimicry attacks.

• The attacker who uses at least the same number of antennas as the receiver's antennas can successfully initiate the mimic attack. It is not easy to identify mimicry attacks.

• Less security against mimicry attacks

4. PROPOSED SYSTEM

If the number of receiving antennas of the receiver is larger than the number of transmitting antennas of the attacker, the receiver can detect the counterfeit attack. There is the structure of the connection signature, which is referred to as the time-synchronized connection signature. The time-synchronized connection signature integrates cryptographic protection and time factor protection into the properties of the wireless physical layer and provides a practical and efficient solution for authenticating wireless signals of the physical layer. Mimicry attack and demonstrates the efficiency of time. - Synchronized connection signature for physical layer authentication.

4.1 ADVANTAGES

- It is very safe against mimicry attacks.
- Easily identifiable mimicry attacks and offers more protection.
- We can demonstrate a large number of experiments to demonstrate both the feasibility of facial expression attacks and the efficiency of the time-synchronized binding signature.

4.2 BLOCK DIAGRAM

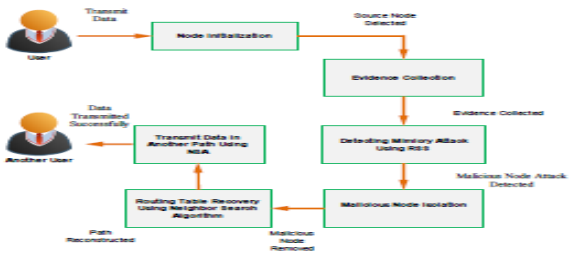


Fig. -1: Functional diagram of our proposed method

4.3 Node Initialization

In this diagram, multi-position users are requesting files from nodes on delay tolerant networks, and the user can access them from their vulnerable nodes. Compromised nodes are caught by the adversary in order to exploit them and take security measures. The adversary can physically capture and compromise the nodes and then carry out a variety of attacks using those compromised nodes. The key idea of our scheme is to detect untrusted zones and perform software certification for the nodes in those zones to detect and revoke them.

4.4 Collection of Evidence

In this module we can collect the evidence of the attacking node. Mimic attack alert. In this module, the intrusion timestamp provides an attack warning with a trustworthy value. Then RSS runs to find out how many changes to the routing table are caused by the attack.

4.5 Detection of A Mimetic Attack

Route table recovery includes recovery of local route tables and recovery of global routes. Local routing recovery is performed by the victim nodes, who detect the attack and automatically retrieve their own routing table. Global routing recovery involves sending routing messages recovered by victim nodes and updating their routing table based on routing information corrected in real time by other nodes in the delay tolerant network.

4.6 Isolation of Malicious Knots

Node isolation can be the most intuitive way to prevent new attacks from being launched by malicious nodes on the delay tolerant network. To perform a node isolation response, the malicious node's neighbors ignore the malicious node by not sending packets. This. On the other hand, a binary node isolation response can negatively impact routing operations and cause even more routing damage than the attack itself.

5. RESULTS AND DISCUSSION

In this project we identify the mimicry attack against existing signature schemes for wireless connections, then extend the mimicry attack to MIMO systems and come to the conclusion that the attacker using at least the same number of antennas as the receiver antennas

is the mimicry -Can initiate the attack successfully.

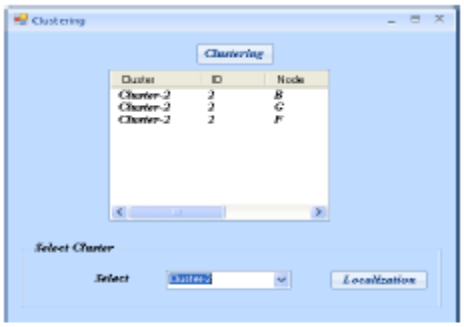


Fig 2 Node Initialization

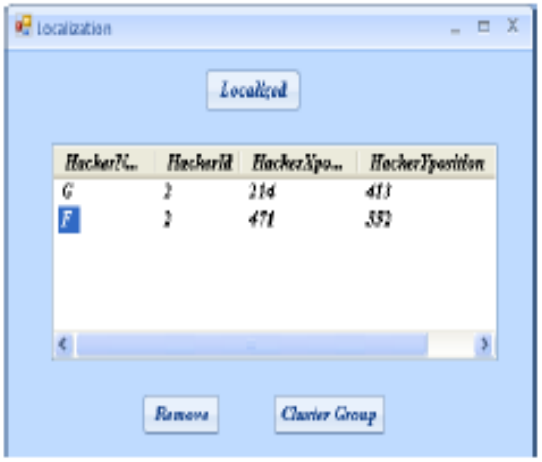


Fig 3 Detection of A Mimetic Attack

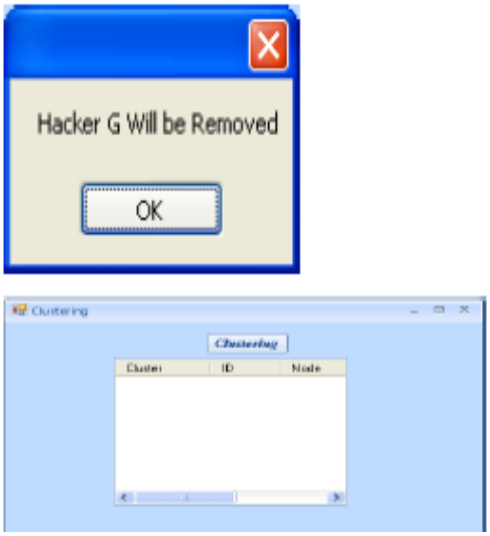


Fig 4 Isolation of Malicious Knots

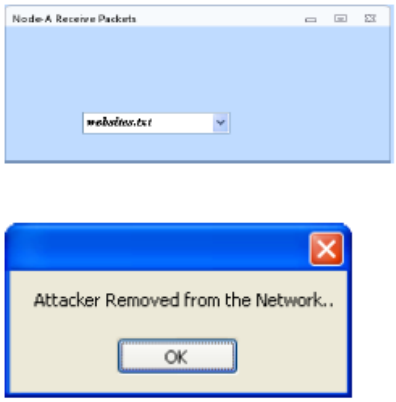


Fig 5 Removal of Attacker from Network

6. CONCLUSION

To defend against the mimicry attack, we proposed the new construction of the time-synchronized connection signature by incorporating cryptographic protection and taking time into account in the properties of the wireless physical layer. We also performed a large number of experiments to demonstrate both the feasibility of mimicry attacks and the effectiveness of time-synchronized link signing.

REFERENCES

1. R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, “Device identi- fication via analog signal fingerprinting: A matched filter approach,” in Proc. 13th Annu. Symp. Netw. Distributted Syst. Secur. (NDSS), 2006, pp. 1–11.
2. D. B. Faria and D. R. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in Proc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 43–52.
3. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identifi- cation with radiometric signatures,” in Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 116–127.
4. L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, “Identifying unique devices through wireless fingerprinting,” in Proc. 1st ACM Conf. Wireless Netw. Secur. 2008, pp. 46–55.
5. N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in Proc. 13th Annu. ACM Int. Conf. Mobile Comput. Netw. 2007, pp. 111–122 .

PSEUDO CODE MINING AND ALGORITHM PROCEDURES FOR INDEXING

Shaik Sulthana Aziya[1]., B.Shruthika [2]., B.Jahnavi [3]., B.Jhansi [4] .,B.Priyanka [5].,

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

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Algorithm procedures (AP) and pseudocodes (PC) are an important source of information for scientists, researchers, developers, scientists and innovators in various areas of technology. Relevant algorithm and pseudocode procedures are not readily available for your analysis and require more effort and time for research. Different algorithms and pseudocode procedures are published in national and international journals every year. Hence, finding efficient and relevant pseudocode algorithms and procedures becomes difficult as efforts are required to compare and analyze them to determine which is most efficient. However, the likelihood of obtaining relevant and efficient algorithm and pseudocode procedures is lower. Appropriate extraction techniques must be used to solve these problems. These techniques include knowledge discovery from the Internet and research articles available in national and international journals in order to obtain the most appropriate match for the user's input requirement. For this purpose, the input request is accepted, the indexing is carried out using suitable mechanisms and the most relevant algorithm procedures and pseudocodes are listed. In addition, the user has the function of downloading algorithm procedures and pseudocodes. Therefore, algorithm procedures as well as pseudocode extraction and analysis become an important part of this implementation.

Keywords* : *extraction, indexing, regular expression, analysis, PDFtoTEXT.

1. INTRODUCTION

In computer science, algorithm procedures (AP) and pseudocodes (PC) are an important source of information for the development and analysis of various applications. These algorithm and pseudocode procedures are used by scientists, researchers, developers, scientists and innovators in various fields of technology. Access points and PCs are efficient methods that contain a finite set of instructions that produce the desired output in finite time and spatial complexity. Different algorithms and pseudocode procedures are published in national and international journals every year. Standard algorithms and pseudocodes are available in various research articles, manuals, encyclopedias, Wikipedia, etc. [1] As new algorithms and pseudocodes are published every year, new relevant algorithms and pseudocodes are increasingly sought. It is not possible. Hence, the user needs to consult many research articles. Therefore, efficient and relevant algorithmic and pseudocode techniques become difficult for research as efforts are required to compare and analyze them to determine the most efficient ones. However, the likelihood of obtaining relevant and efficient algorithm and pseudocode procedures is lower.

2 RELATED WORK

In addition to the popular web search engines such as Microsoft's Google5 and Bing6, several vertical search engines have been proposed. CiteSeer7, now CiteSeerX, was developed as a digital scientific literature library and search engine that automatically crawls and indexes scientific documents, especially in the field of computer and information science [2].

Liu et al. Introduced TableSeer, a tool that automatically identifies and extracts tables in digital documents [3]. They used a ranking algorithm based on the TableRank custom vector space model to classify the search results. The CiteseerX suite includes an implementation of TableSeer that extracts and searches for tables in the CiteSeerX document repository. The BioText8 search engine, a specialized search engine for biological documents, also offers the option of extracting figures and tables and making them searchable [4]. Khabsa et al., Describe AckSeer, a recognition search engine that extracts, clarifies, and indexes over 4 million named entities from 500,000 document confirmations in CiteSeerX [5].

3 PROPOSED SYSTEM

In this article, the system will be developed to extract access points and PCs from the research article and from the web. The extracted APs and PCs are saved in the database. Access points and PCs are then scanned based on application complexity, time and space. The user has to give an input request in the form of the keywords AP and PC. The system displays affected APs and PCs using the appropriate indexing mechanisms, making downloading easier for APs and PCs.

3.1 Modules

There are basically five modules in the system:

1. Convert PDF to Text.

2. AP and PC extraction.
3. Analysis.
4. Indexing.
5. Display the AP and PC.

3.2 Converting PDF to Text.

Extracting AP and PC from PDF is a tedious task, so research documents are first converted to text format using PDF TO TEXT libraries. Therefore, the converted text is used to extract the algorithm procedures and pseudocodes.

3.4 Extraction from AP and PC.

During the extraction, access points and PCs are extracted using different techniques. These techniques include regular expression and machine learning. In the research article, the keywords match using regular expressions. The keywords are like "algorithm", "pseudocodes", "start", "end", "step", "start", "initialization" etc. As soon as the keyword matches, the marked APs and PCs are saved in the database.

An algorithmic procedure consists of a series of descriptive algorithmic instructions and differs from a PC in the following ways:

1. Writing style. PCs are often written in a programming style with details left out. Symbols, Greek letters, math operators, and programming keywords (such as "to", "start", "end", "return", etc.)Access points are incapable of expressing complex nested loops and are less precise than personal computers.
2. Position in documents. PCs are usually not part of the running text. They can appear anywhere in the documents. For this reason, most PCs have identifiers that can be referenced in the context of the document. These identifiers include titles, function names.

3.5 AP and PC analysis.

In the analysis module, the access points and PCs stored in the database are analyzed according to the complexity of the application, time and space. In this analysis phase, PAs and PCs therefore determine which PAs and PCs are better, worse, or average.

3.6 AP and PC indexing.

The indexing mechanism indexes the scanned APs and PCs so that affected APs and PCs are displayed to meet user needs. And this is how APs and PCs can be downloaded.

4 SYSTEM ARCHITECTURE.

The system architecture is shown below:

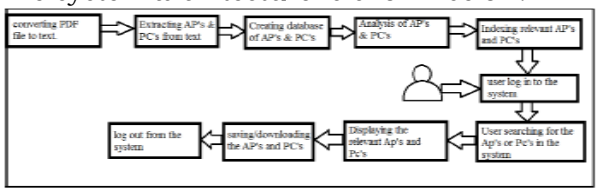


Fig.1 System architecture

The architecture diagram gives the overall representation of the modules and their execution processes. There are a total of five main modules, which are structured in the system as follows:

1. Convert a PDF document to text.
2. Extraction of algorithm procedures and pseudocodes.
3. Save the extracted data in the database.
3. Analysis of algorithm and pseudocode procedures.
4. Indexing of algorithm procedures and pseudocodes.
5. Visualization of the most important pseudocode algorithms and procedures.
6. Download the algorithm procedures and pseudocodes.

Access points and PCs in research articles and on the Internet are accessed and stored in the database. The APs and PCs are then analyzed by calculating the complexity of time and space and the applications are indexed to get the relevant results.

4.1 FIND OUT THE RESULTS.

4.1.1 Convert PDF document to text

The system converts the PDF document from which the algorithm procedures and pseudocodes are extracted into text. The results are displayed in the following screenshot format:

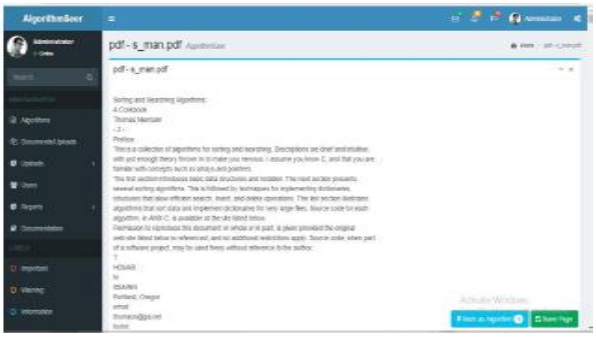


Fig.2.PDF TO TEXT.

4.1.2 Evaluation of the algorithm procedures.

Figure 3 Algorithm procedure

Access points are recognized using writing styles such as start, start, end, and so on. The recognized algorithm procedures are extracted from the file using the regular expression. The user searches for the algorithm procedures using the algorithm keywords.

5 RESULT AND EVALUATION

PCs are recognized by writing styles such as "int", "begin", "for", "end" and so on. The recognized pseudocodes are extracted from the file with the regular expression. The user searches for the pseudocodes using the pseudocode keywords.

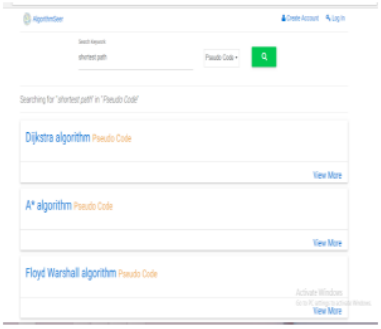


Figure 4 Pseudocodes

The most relevant algorithms and pseudocodes are listed. Algorithm procedures and the extraction and analysis of pseudocodes become an important part of this implementation, which makes searching easy and relevant for users.

6 CONCLUSION

Algorithm and pseudocode techniques play an essential role in research and development centers, academics, innovators, scientists, etc. This system is a research technique for extracting and analyzing relevant and efficient algorithm (PA) and pseudocode (PC) techniques from research articles and the internet. Since there are several options available, choosing the most suitable is a daunting task. Therefore, the system uses an indexing mechanism to indicate the most relevant algorithm procedures and pseudocodes. This reduces the time and personnel expenditure. Therefore, the system offers an efficient and relevant search engine to search for the appropriate pseudocode algorithm and procedures with their temporal, spatial and application complexity.

REFERENCES

1. Y. Liu, K. Bai, P. Mitra, and C. L. Giles, “Tableseer: Automatic table metadata extraction and searching in digital libraries,” in Proc. 7th ACM/IEEE-CS Joint Conf. Digital Libraries, 2007, pp. 91–100.
2. M. A. Hearst, A. Divoli, H. Guturu, A. Ksikes, P. Nakov, M. A. Wooldridge, and J. Ye, “BioText search engine: Beyond abstract search,” Bioinformatics, vol. 23, no. 16, pp. 2196–2197, 2007.
3. ”AlgorithmSeer: A System for Extracting and Searching for Algorithms in Scholarly Big Data.”,Suppawong Tuarob, Sumit Bhatia, Prasenjit Mitra.
4. H. Li, I. Councill, W.-C. Lee, and C. L. Giles, “Citeseerx: An architecture and web service design for an academic document search engine,” in Proc. 15th Int. Conf. World Wide Web, 2006, pp. 883–884.
5. M. Khabsa, P. Treeratpituk, and C. L. Giles, “Ackseer: A repository and search engine for automatically extracted acknowledgments from digital libraries,” in Proc. 12th ACM/IEEE-CS Joint Conf. Digital Libraries, 2012, pp. 185–194.
6. H.-H. Chen, L. Gou, X. Zhang, and C. L. Giles, “Collabseer: A search engine for collaboration discovery,” in Proc. 11th Annu. Int. ACM/IEEE Joint Conf. Digital libraries, 2011, pp. 231–240.

ROBUST VISUAL OBJECTS TRACKING IN VIDEO VIA SVM AND FEATURE MAPPING SYSTEM

Sanjeev Sagar, K[1]., P.Ravalika [2]., P.Vasavi [3]., P.Anjali [4] ., P.Spandhana [5].,

1Assistant 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, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

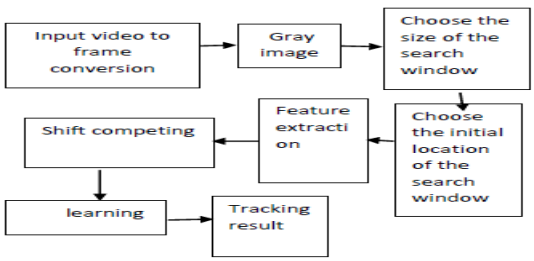
Abstract— Visual tracking is a difficult process due to variations caused by various factors such as object deformation, occlusion, scaling, and changes in lighting. In our proposed system, we tend to overcome these drawbacks by using an expectation maximizing algorithm and a support vector machine. With this algorithm, we can improve the accuracy of tracking an object or a person from a video. This monitoring model is better in terms of efficiency and robustness. This tracker maintains a speed of around 45 fps.

Keywords : extraction, indexing, regular expression, analysis, PDFtoTEXT. Maximizing Expectations, Supporting Vector Machine, Positive Models, Occlusion Detection, Tracking, Precision.

1. INTRODUCTION

Tracking objects visually is a fundamental problem in image processing. It has various applications such as motion analysis, video surveillance, human-computer interaction, and robot perception. Although a lot of research is being done to develop this process, it remains challenging due to some factors such as appearance, change in pose, occlusion, etc. Hence, it is necessary to develop a better representation of the features in order to obtain more efficient tracking models. The intuition behind SFA is related to the assumption that the information in a signal changes slowly, rather than suddenly. Note that there is usually a lot of variation in a signal (caused by noise). However, it is the seldom varying properties that characterize the separation between changes in information. SFA extracts these characteristics by selecting the important attributes that change the least **over time.**

2. BLOCK DIAGRAM



3 MODULES

- Select the target image in the opening image
- Extraction of functions
- Follow up

3.1 SELECT THE TARGET IMAGE OF THE INITIAL FRAME:

We summarize the generation of dynamic image tracking as the input sequence of color images. We'll start by cutting out the area of a target in the source image. This window size is fixed. Average the data in the window.

3.2 EXTRACTION OF FUNCTIONS

In the marked object given to the algorithm, the properties are calculated using the expectation maximizing algorithm.

3.3 MONITORING

In each frame the features are calculated, this is machine learned, the object is recognized and this is tracked in each frame using support vector machine classifiers.

4 SOFTWARE USED

- MATLAB 8.3.0.532 (R2014a)

MATLAB is a matrix laboratory used to solve many technical computing problems. Used to access the matrix software. It is used for simulation, modeling and prototyping.

5 OCCULISION DETECTION AND MODEL UPDATE:

At the time of the follow-up examination, the target with slight occlusion or no occlusion is represented by positive models. If the object has a strong occlusion, it will be represented not only by positive models, but also by

negative models. The occlusion is detected according to the criteria for using or not using negative models to represent the target. If more negative models are used to reconstruct the goal, it means that the goal is seriously cast. If more negative models are used to reconstruct the target, it will be used for the error detection rate. If an occlusion is detected, the negative model is updated every 5 images. No positive model is updated at this point. If the reconstruction error in the positive sample is less than the limit of 0.5, the current tracking result is a good candidate to represent the target. After that, the result of the follow-up is added to the positive models. After that, the best tracking results are added continuously, making the positive model bigger.

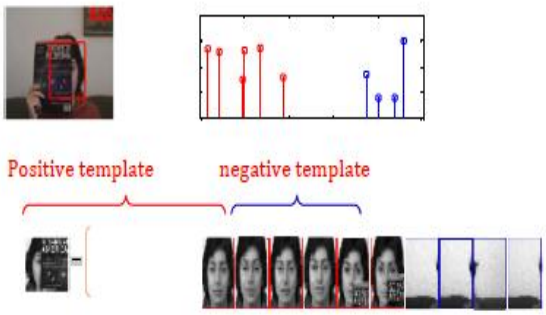


Figure 1: The representation of a hidden target is represented by positive and negative models.

6. QUALITATIVE EVALUATION:

6.1 Intensive occlusion:

When the target is obscured, our proposed system finds an object perfectly in terms of rotation and position. However, the previous IVT L1APG and MTT method cannot locate an ATD tracking target in frames. Our suggested method is more accurate than the previous methods.

6.2 Deformation and change of rotation:

The target is easy to get confused as it moves and changes its appearance. However, our proposed system could easily identify the object even if the appearance of the target changes. Only the system we offer can track an object to a certain extent in sensitive background conditions and poor lighting.

6.3 Abrupt movement and shake of the camera:

It's hard to predict an animal and a human when both experience sudden movements and the camera shakes. Most trackers cannot track the target because of a large gap in an animal or human's sequence.

7 RESULTS

Here developed learning tools to model the temporal relationship between cortical responses, which can further improve tracking accuracy. Track people through multiple cameras from different angles. In video surveillance, it took billions of hours to track a person or object from video. Human labor is expensive. In our work we use computer-aided monitoring that takes place automatically.

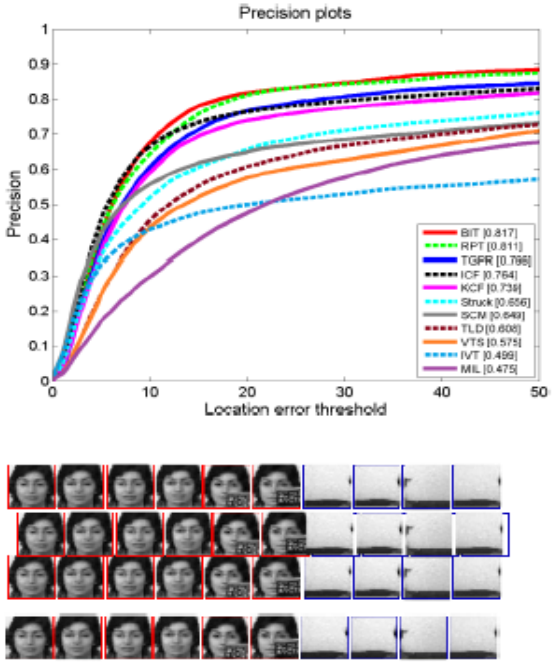


Fig 2: Precision Plot

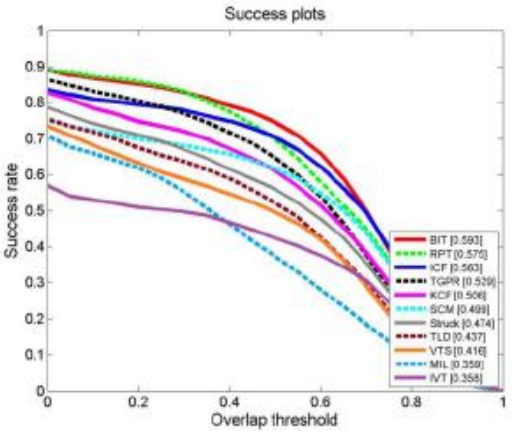


Fig 3: Succes Plot

8 CONCLUSION

With this method, we can improve the accuracy of tracking an object or a person from a video. In the above method, we cannot track an object or person more closely because of the occlusion and distortion in a video. By using the expectation maximizing algorithm and the support vector machine, we get more precision.

REFERENCES

1. L. Sevilla-Lara and E. Learned-Miller, "Distribution fields for tracking," in Proc. Comput. Vis. Pattern Recognit., Jun. 2012, pp. 1910–1917.
2. T. B. Dinh, N. Vo, and G. Medioni, "Context tracker: Exploring supporters and distracters in unconstrained environments," in Proc. Comput. Vis. Pattern Recognit., Jun. 2011, pp. 1177–1184.
3. K. Cannons, "A review of visual tracking," Dept. Comput. Sci. Eng., York Univ., Toronto, ON, Canada, Tech. Rep. CSE-2008-07, 2008.
4. D. Comaniciu, V. Ramesh, and P. Meer, "Kernel-based object tracking," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 5, pp. 564–577, May 2003.
5. J. F. Henriques, R. Caseiro, P. Martins, and J. Batista, "High-speed tracking with kernelized correlation filters," IEEE Trans. Pattern Anal. Mach. Intell., vol. 37, no. 3, pp. 583–596, Mar. 2015.
6. H. Zhou, Y. Yuan, and C. Shi, "Object tracking using SIFT features and mean shift," Comput. Vis. image Understand., vol. 113, no. 3, pp. 345–352, Mar. 2009.
7. K. Zhang, L. Zhang, and M.-H. Yang, "Real-time compressive tracking," in Computer Vision—ECCV. Berlin, Germany: Springer, 2012, pp. 864–877.

GBRT MACHINE LEARNING FRAMEWORK FOR SMART CACHING OF DATA OBJECTS FOR ANDROID WEB BROWSERS

Ch.Mahesh[1] ., P.Mounika [2]., P.Vinitha [3]., P.Nikitha [4] ., R.Srivalli [5].,

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

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Battery life, which is one of the most important user experiences for mobile devices, severely limits the functional design of hardware architecture and applications. Among all aspects of energy saving for mobile devices, the design of energy efficient applications is one of the main areas that have yet to be fully explored. In this project work, we advocate the design of energy efficient mobile applications as there is a large gap for energy saving in applications and we believe that this is a promising area for energy saving. Energy in mobile devices. To aid in the design of energy-conscious mobile applications, we propose a framework called GBRT, with the aim of adding a power adjustment layer by providing a set of APIs and adjustment guidelines.Our proposal with two apps for Android shows that GBRT can save a lot of energy by enabling apps to change app mode and increase energy efficiency. In addition, our solution can reduce the loading time of websites and increase the network capacity.

Keywords* : *web browsers, mobile computing, wireless communications, portable devices.

1. INTRODUCTION

The smartphone is one of the most important applications for various purposes. Smartphone-based internet surfing is mostly a technique or pattern provided by a smartphone. There are various smartphones on the market, but they used a lot of power for their action or at the time of downloading from the website. There is a lot of research going on into the energy consumption of smartphones. And they only focused on the power consumption of the components of the smartphone, such as B. Screen, wireless interface and WLAN interface with high power consumption. In order to reduce power consumption, the radio resources must be controlled. UMTS technologies mainly focus on these issues. They are used to control radio resources and their time values at the time of resource release. A big advantage of our system is to reduce the latency in the transmission of data that arrives before the timer. It will expire because a connection is still available between the backbone and the smartphone. In particular, our diagram defines energy efficiency as mobile devices are usually charged with batteries of limited capacity. Although energy savings for mobile devices were examined, the power consumption in bandwidth aggregation was not defined.

2. LITERATURE SURVEY

In modern web applications, style formatting and layout computation are often a significant part of rendering time for local web pages. This document introduces two new caches, Smart Style Caching and Layout Caching for Web Browsers. They cache stable style and layout data for Document Object Model (DOM) elements and are directly applied without recalculation when the same data is subsequently processed, possibly on different visits to a web page. Redundant calculations in the style format and in the layout calculation could be avoided, which would lead to more efficient rendering of local web pages. The proposed cache schemes remain applicable and effective even if the DOM structure or the style rules of a website are changed. For overall performance in processing local web pages, web servers, and networks, our caching schemes improved by up to 56% when browsing these websites on a desktop computer and by up to 60% when browsing on a netbook.

3 PROPOSED SYSTEM

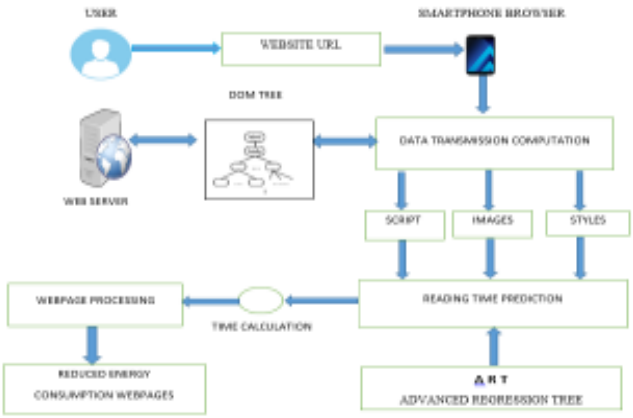


Fig 1 System Model

We are approaching the problem of energy consumption when surfing the Internet on smartphones with two new techniques. First, we change the order in which the web browser computes when a web page is loaded. There are various calculations involved in loading a web page, such as: B. parsing HTML, running JavaScript code, decoding images, formatting styles, layout, etc. These calculations can generally be divided into two categories, depending on whether they are generating new data transfers from the web server or Not. So that the web browser can first perform the calculations that generate new data transfers and retrieve that data. The web browser can then put the wireless radio interface into a power-saving mode, release the radio resource and then perform the remaining calculations, which take 40-70% of the processing time to load the web pages. Therefore, a large amount of power and radio resources can be saved.

3.1. Calculation of the data transfer

In the current smartphone web browser, two types of calculations are assigned to each incoming object. The first type is the computation that generates new data flows, e.g. For example, parsing HTML and CSS files and executing JavaScript code called data flow calculation. The second type is the calculation that does not cause data transmission. This type of calculation is used to design the website, e.g. B. Image decoding, style formatting, page layout calculation, and page rendering which is referred to as page layout calculation.

3.2. GBRT

A machine learning-based approach to predicting the user's reading time, which we can use to decide whether the smartphone should switch to IDLE. Because different users have different reading patterns, we created the prediction engine for each user individually. This relies on machine learning to predict users' reading time. On this basis, we can decide whether the smartphone should switch to IDLE. Because different users have different reading patterns, we'll create the prediction engine for each user individually.

3.3. Conscious use of energy

We introduce our energy-based focusing algorithm, which has two different modes: the delay-controlled mode, which optimizes the delay, and the energy-driven mode, which optimizes the performance. Note that an incorrect entry in the INACTIVE status can increase power consumption and delay data transmission. In delay mode, if the expected read time (Tr) is less than T d, new data transfers can occur during the FACH state and therefore the smartphone does not go into idle mode to avoid extending the data transfer time.

3.4 Algorithm

For optimal preload

To grab:

1) The list of "n" hyperlinks on the current webpage.

2) Minimal support ie "minsup" which controls the number of hyperlinks to be searched beforehand.

3) List of custom keywords

Production:

1) The optimal list of hyperlinks to be searched beforehand; H. "L", a large amount of hyperlinks if support> = download minute variables:

1) "n": Integer that contains the total number of unique keywords

2) i1, i2 ---------- in a series of unique keywords from the hyperlink list

3) "k": whole number

4) "Termination": Boolean value

5) "support []", which contains the keyword support value calculated from the formula

6) "C" which contains the set of keywords which are candidates for pre-extraction and C1, C2 ---------- Ck is the set of candidate keywords which are a set of keywords of length contains k with your support value. Optimal_ prefetching () {algorithm

1. Count the unique individual keywords from the hyperlink list that match the custom list, parse all the hyperlinks once and pronounce them as "n".

2. for j = 1 an do {calculate the support [ij] = count (ij) / m by scanning all hyperlinks once and counting the number of hyperlinks in which the keyword ij occurs (i.e. count (ij)) . }}

3. Now create the keyword set Candidate1, ie C1, which is the keyword set i1, i2 ---------- with its supporting value.

4. for j = 1 year do {Calculate the L1, which contains the subset of the keywords of C1, where support (ij)> = minup.}

5. Let k = 1 and termination = false

6. Repeat steps (a) through (e) until completion = true {a. Let Lk + 1 = empty. B. Create the candidate keyword set (k + 1), i. H. Ck + 1 by combining the members of Lk by selecting and expanding the keyword set k with another keyword so that the keyword set is unique and no keyword is repeated in each row. Consider only these k + 1 keywords as keywords of Ck + 1, so that every subset of size k appears in Lk. D. Scan the hyperlinks once and calculate the

support for each member of Ck + 1. If the support for a member of Ck + 1> = minsup, add that member to Lk + 1. Mi. If Lk + 1 is empty, the termination = true, otherwise k = k + 1}
7. Lk now contains the list of previously searched hyperlinks.
8th end.}
Algorithm
For an energy conscious approach:
1. Open a web page.
2. The data transfer calculation is carried out.
3. The design calculation is completed.
4. Collect the features x = {x1, • • •, x10}
5. The website opens
6. Wait α seconds.
7. Obtain Tr from the predictive model with x
8.if (Tr> Td) OR (Tr> Tp AND mode == power) then
9. Switch to the inactive state
10th end

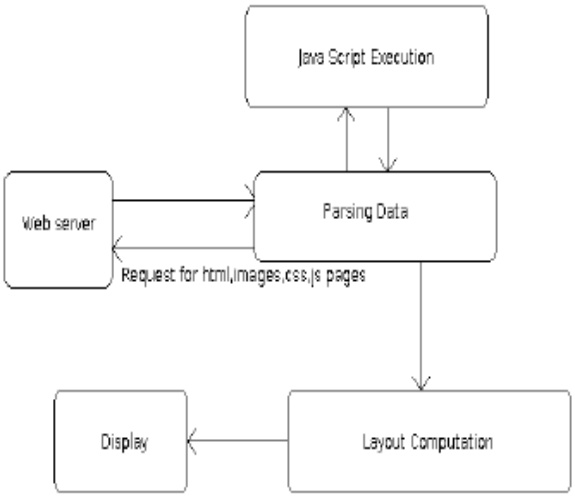


Figure 2 Block Diagram

4 RESULT AND DISCUSSION

In our proposed system, data transfers are carried out in an energy efficient manner via WLAN and 3G interfaces. In this article, we will focus on the problem of power consumption while browsing on smartphone using two new techniques. In the first techniques, we get the order of the web browser computation at the time of loading web pages. There are various calculations involved in loading a web page, such as: B. parsing HTML, running JavaScript code, decoding images, formatting style, layout, etc. These calculations fall into two categories, depending on whether new data streams are being created by the web server or not. . Therefore, we want to separate these two types of calculations so that the web browser can first do the calculations that are used to create new data streams and retrieve that data. The web browser can then put the 3G radio interface into a power-saving mode, release the radio resource and then perform the remaining calculations, which take 40% to 70% of the processing time to load the web pages. Therefore, a large amount of power and radio resources can be saved. In particular, our diagram defines energy efficiency as mobile devices are usually charged with batteries of limited capacity. Although energy savings for mobile devices were investigated, the power consumption in bandwidth aggregation was not defined. In our proposed system, data transmission takes place via WLAN and 3G interfaces in the form of energy efficiency

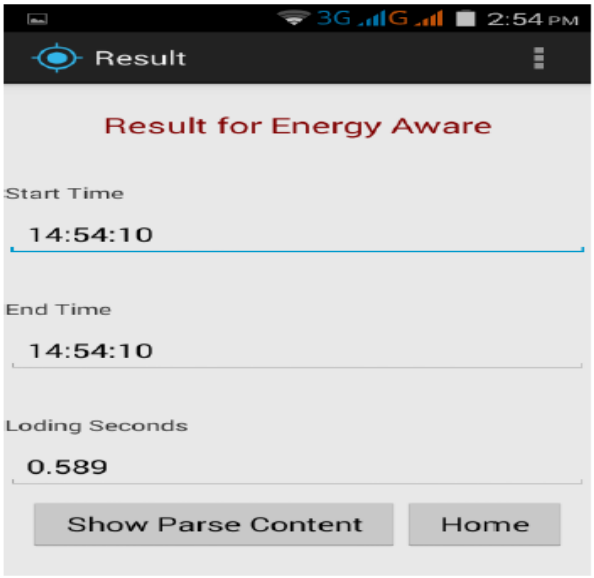


Figure 3 : Result for Energy Aware

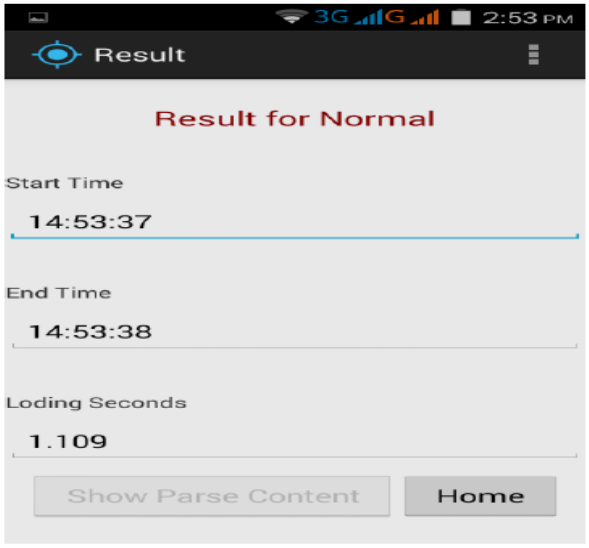


Figure 4: Result for Normal

5 CONCLUSION

In this intelligent data caching-caching for web browser we first rearrange the calculation sequence to load the web page so that the web browser can first perform the calculations that generate new data transfers and retrieve this data. Since smartphones only have limited computing power, we offer a cost-effective prediction algorithm based on gradient-fed regression trees. In addition, our approach can also increase the capacity of the network as the radio resource can be released earlier.

REFERENCES

1. M. Dong and L. Zhong, "Chameleon: A color-adaptive web browser for mobile OLED displays," in Proc. ACM 9th Int. Conf. Mobile Syst., Appl., Serv., 2011, pp. 85–98.
2. E. Shih, P. Bahl, and M. J. Sinclair, "Wake on wireless: An event driven energy saving strategy for battery operated devices," in Proc. ACM 8th Annu. Int. Conf. Mobile Comput. Netw. 2002, pp. 160–171.
3. F. R. Dogar, P. Steenkiste, and K. Papagiannaki, "Catnap: Exploiting high bandwidth wireless interfaces to save energy for mobile devices," in Proc. ACM 8th Int. Conf. Mobile Syst., Appl., Serv., 2010, pp. 107–122.
4. J. Flinn and M. Satyanarayanan, "Managing battery lifetime with energy-aware adaptation," ACM Trans. Comput. Syst., pp. 137– 179, May 2004.
5. J. Sorber, N. Banerjee, M. D. Corner, and S. Rollins, "Turducken: Hierarchical power management for mobile devices," in Proc. ACM 3rd Int. Conf. Mobile Syst., Appl., Serv., 2005, pp. 261–274.
6. E. Rozner, V. Navda, R. Ramjee, and S. Rayanchu, "NAPman: network-assisted power management for wifi devices," in Proc. ACM 8th Int. Conf. Mobile Syst., Appl., Serv., 2010, pp. 91–106.
7. 3GPP Specification TS 24.008: Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3, Std., Rev. Rel. 9, 2009.

PERSON IDENTIFICATION USING IRIS RECOGNITION USING HYBRID WAVELET TRANSFORM AND ROI

K.Manasa[1] ., G.Harika [2]., G.Sneha [3]., G.Punvitha [4] ., R.Srivalli [5].,

1Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ kondamansa@mrcew.ac.in)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The security and authentication of people is essential in many areas of our lives, and most people need to authenticate their identities on a daily basis. Examples include ATMs, secure building access, and international travel. Biometric identification offers a valid alternative to traditional authentication mechanisms such as ID cards and passwords, while overcoming many of the shortcomings of these methods. Iris recognition is more accurate than any other biometric feature. The goal of this project is to create a functional prototype program that acts as an iris recognition tool, comparing the RED (Ridge Edge Direction) and HWT (Hybrid Wavelet Transform) algorithms for feature extraction in order to implement iris authentication system implementations implemented in MATLAB to be more accurate and useful, which is simple is to use. Our main goal is to develop an application-based system that accurately authenticates everyone. The app-based system provides security for the door of a company or institute by repairing our system, which authenticates everyone and shows the result when the person is authenticated. The door will open automatically. We'll show it in the graphical user interface (GUI). Our goal is to provide the most accurate security system for everyday use.

Keywords : ROT, HWT, authentication, feature extraction, MATLAB..

1. INTRODUCTION

Iris recognition is one of the most accurate methods used today for human-to-human identification [1]. The Iris-based authentication system determines the identity of the user in principle that certain characteristics of the Iris are unique for each person. In recent years, new areas of algorithms have grown.For iris recognition in the area of automated human identification. Real-time automated iris systems have been successfully implemented in several public applications. The researchers tried to develop a system that would allow them to perform iris recognition to work in real time in the application. Therefore, they tried to develop a special system for iris recognition that works at high speed and at low cost. There are four main steps involved in implementing an iris recognition system: 1) image acquisition; 2) preprocessing, including segmentation and normalization; 3) feature extraction that creates an iris model; and 4) comparison of iris patterns and recognition decision (match).

2. LITERATURE SURVEY

2.1 Pretreatment

The analysis of the structural properties of the eyelashes, a method of detecting eyelash closures based on the identification of extreme points, has been explained here. With feature extraction, useful information is retrieved from the iris that is useful for authenticating the person. To create feature vectors, mathematical operations are performed on the input image and the results are used to create the feature vector when the image is normalized. In our methods, the upper right part of the iris is used by unrolling it with the Daugman rubber sheet model for normalization. A feature vector must be compared to the database to identify the person it belongs to.

3 PROPOSED SYSTEM

The proposed methods use the sliding window technique. The methods used are as follows:

1) Method 1: Average threshold

2) Method 2: Threshold of the mean through median

2.3 Iris Match / Authentication

1) Fragile bit removal and Hamming removal:

The proposed fusion between the Hamming distance (HD) and the brittle bit distance (FBD) works well as the Hamming distance alone.

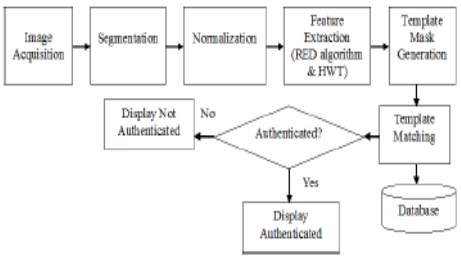


Fig 1 Proposed system block diagram

Step1: Detection of eyelash closures using endpoint identification: In this document, only the detection of the edges of the inner and outer iris was explained in detail. It doesn't explain the general iris recognition process.
Step 2: Improved Iris Recognition Based on Image Fitting and Hammer Distance - In this article, the iris segmentation is done using the Hough transform, the iris feature extraction using the Gabor filter and the corresponding pattern using hammering which did not give an efficient result.
Step 3: New Recognition Methods for Human Iris Patterns: In this article, feature extraction is performed using thresholding techniques and the Hamming distance is used for pattern matching, where n was not an accurate result.

The first step in iris recognition is to capture the image. Choosing a good, clear and noise-free image eliminates the de-noise process and prevents miscalculations. Once the image has been obtained, several pre-processing steps are performed on the image. It includes segmentation, normalization (conversion from polar to rectangle) and the creation of template and mask by applying the RED algorithm to the rectangular template. This model is compared to the database using Hamming distance (the main method of matching iris) and the Match ID is displayed.

3.1 Segmentation

The segmentation process is used to isolate the iris from the captured image. The iris region lies between the outer boundaries of the iris and the pupil. The segmentation process is the most important factor in iris recognition. If the recognition of the pupil and the edge of the iris is precise, the identification will be more accurate. Then it will be roughly in the iris area as shown in the picture.

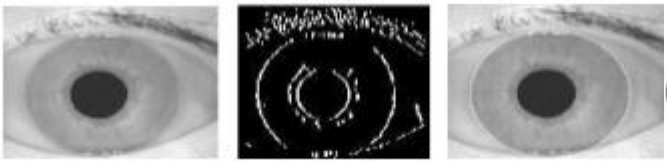


Figure 2. a) Original image b) Image after clever edge detection with the circular Hough transform. c) Detection of the iris with a Hough Iris transformer.

The first step is to use an edge finder, which is a technique for locating edges. The edge finder is used to locate the edge of the iris and the edge of the pupil. The Canny Edge Algorithm is used here, which is the most efficient method of detecting edges. It depends on the strength and intensity value of the pixel that detects the edge of the image. After the border crossing is complete, the next segmentation step is to use the Circular Hough Transform (CHT), which is used to detect circles of the iris and pupils.

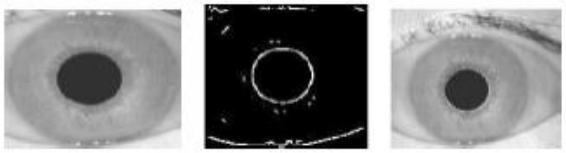


Figure 3. a) Adjustment image taken from the base of the original image in the center of the iris. B) The sophisticated pupil edge detector. C) Hough transformer pupil detection.

After recognizing the border of the iris, it is time to recognize the border of the pupil, but first mask the captured image and extract only the image of the iris, as shown in the figure, because the pupil is always inside the iris. This shape is used to reduce the processing time of Hough space because the circular Hough transform is a "raw force" and many pixels try to locate the pupil there. The mask reduces the pixel sought by the pupil circle [6]. Use the same process to locate the iris circle and apply a sneaky edge finder to mask the image. Then apply the CHT and find the large circle generated from the sneaky edge image (see picture).

3.2 Standardization

During normalization, the iris is converted from the polar coordinate to the rectangular coordinate. The next step is to convert from polar to rectangular. The rectangular transformation is applied to the area between the pupil radius and the iris radius. This process generates the rectangular model as shown in Figure 4.

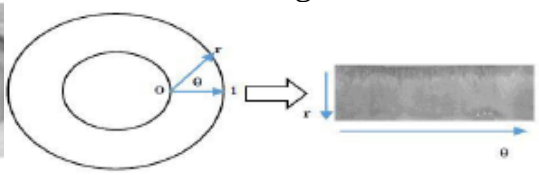


Figure 4. Converting polar models to rectangular models

The process of converting the iris image to a rectangular model is performed using the common transformation from polar coordinates to rectangular coordinates. This

process is known as normalization. Remaps each pixel in the iris realm to correspond to polar coordinates (r, θ), where "r" is in the unit interval [0, 1] and "θ" is the common angular size that is cyclic over [0, 2π]. . This is called the homogeneous rubber sheet model, which was first used by Daugman [6]. The rubber plate model takes into account pupil dilation and size inconsistencies in order to produce a normalized representation with constant dimensions.

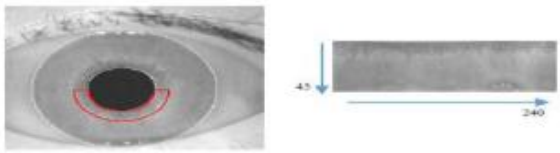


Figure 5. a) Take only the portion of the lower ring of the iris border to create a rectangular iris that will be applied to the RED algorithm. b) Rectangular iris with a height of 45 and a width of 240 of the lower part of the iris.

Typically, the rectangular iris is generated with a radial resolution of 90 pixels and an angle of 480 pixels to produce 90 x 480 iris patterns. The area of the iris surrounded by the red line is chosen to become a rectangular iris, as shown in Figure (5). This rectangular iris contains only a quarter of the iris area, which has enough properties to allow authentication between users. This rectangular iris was chosen because it does not contain any noise that could affect the recognition results. The size of this area in pixels is 45 * 240 pixels.

4. EXTRACTION OF FUNCTIONS

4.1 Algorithm for the direction of peak energy direction (ROT)

The Ridge Energy Direction (RED) algorithm is used for iris recognition. The feature extraction is based on the direction of the peaks that appear in the image. The RED algorithm indicates that the iris of the rectangle is filtered through a bidirectional filter to determine the presence of peaks and their orientation. The filter processing is repeated twice on the rectangular iris, one with a vertical filter and the other with a horizontal filter, as shown in the figure. The 9 * 9 RED filter was selected for both rectangular models [5].

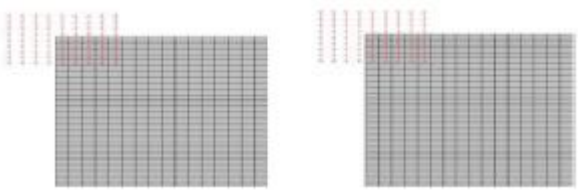


Figure 6.a) Size of the vertical filter RED 9 * 9. B) Size of the horizontal filter RED 9 * 9.

As soon as the rectangular iris model has passed through two filters, two images are generated from the horizontal and vertical dimensions, one of which is the result of the vertical filter with the rectangular iris model and the other is the horizontal filter with the rectangular iris model. . The output of each filter is compared and a "1" for strong vertical content or a "0" for strong horizontal content is assigned for each pixel.

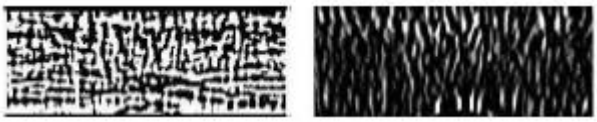


Figure 7. a) Result of the vertical template of the vertical filter with the first iris template. b) Result of the horizontal model of the horizontal filter with the first iris model.

4.2 Hybrid wavelet transformation

In this HWT a combination of discrete cosine transformation and Harr wavelet transformation is formed. A discrete cosine transform (DCT) expresses a finite sequence of data points as the sum of cosine functions that oscillate at different frequencies. DCTs are important for the lossy compression of audio, images, and the digital clarification of PDE.

The DCT algorithm has been used to improve performance to remove noise and insert missing information in regions with sensitive sizes and better visual quality. The Harr wavelet transform is a kind of discrete wavelet transform

$$F(u,v) = \frac{C_u}{2}\frac{C_v}{2}\sum_{y=0}^{7}\sum_{x=0}^{7} f(x,y)\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right]$$

With:

$$C_u = \begin{cases} \frac{1}{\sqrt{2}} & if\ u = 0, \\ 1 & if\ u > 0 \end{cases}; \quad C_v = \begin{cases} \frac{1}{\sqrt{2}} & if\ v = 0, \\ 1 & if\ v > 0 \end{cases}$$

The Harr wavelet is a sequence of "quadratic" functions of changed size that are composed of a basis or family of

wavelets. Harr's wavelet performed better than other wavelets in iris recognition.

4.2 Matching models

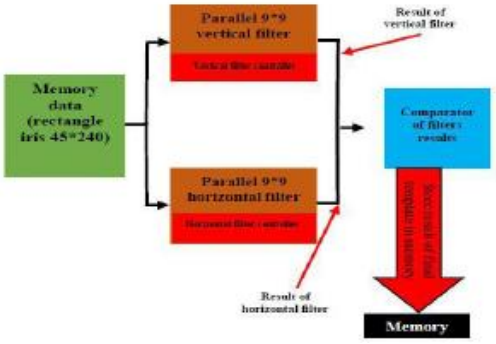


Figure 8. Ridge Energy Direction algorithm process

The model can now be compared with the stored model, using the Hamming distance (HD) as a measure of proximity. The closer the HD is to zero, the more accurate the identification. The closest proximity between two eyes is 0.32 as stated by Daugman [3].

$$HD = \frac{[(Template\ A \times Template\ B) \cap MaskA \cap MaskB]}{[MaskA \cap MaskB]}$$

If model A is the captured image of the iris model and model B is the iris model of the database and the symbol indicates the exclusive or binary operator to detect inconsistencies between the bits that represent the addresses in both models, ∩ is the binary number AND, ‖ • ‖ is a sum, and mask A is the associated binary mask for the captured image model and mask B is the associated binary mask for the database. The denominator ensures that only the required valid bits are included in a calculation.

5. RESULT

Iris template	Size of iris template	Correct matching
Iris template contains feature from the lower part of the eye	90*240 pixel	98.86%
Iris template contains feature from iris that near to the pupil	30*480 pixel	100%

Table 1. Agreement of the iris model and the size result

The iris model has two advantages, one of which is speed as the captured model is small and takes little time to complete the RED process shown in the table. The second advantage is that it is more precise than the anterior iris template. because the area closest to the pupil most of the time lacks eyelids and lashes that are considered noise, while the lower part of the eye may contain eyelids and lashes that result from a mistake.

6. CONCLUSION

The algorithms used for the extraction of iris features are simple and fast algorithms for extracting features from the iris image. The fourth iris region is enough to identify between people because the match between the fourth iris in the database can be successfully recognized and we can get the result. The quarter iris improves the RED algorithm because the time it takes to apply the filter to the entire iris is less than the time it takes to apply the filter to the quarter iris. The algorithm that performs best in terms of time and accuracy may be best for authentication.

REFERENCES

1. Daugman J G, High Confidence Visual Recognition of Persons by a Test of Statistical Independence [J].IEEE Tractions on Pattern Analysis and Machine Intelligence, 1993, Vol. 15, No.11:1148-1161.
2. Gong Chen, Youling Zhou, Iris Location Based on Hough Transform, Journal of East China University of Science and Technology, 2004-04:230-233(in Chinese).
3. Gonzalez,R.C, etc. Digital Image Processing Using MATLAB, Publishing House of Electronics Industry, 2004.5.
4. Thin Iris Region Recognition Using the RED Algorithm, by Safaa S. Omran and Aqeel A. Al-Hillali in Eng. & Tech. journal, vol.34, Part(A), No.5,2016.
5. New Recognition Methods for Human Iris Patterns, by Khalid A. Darabkh, Raed T. Al-Zubi, and Mariam T. Jaludi, MIPRO 2014, 26-30 May 2014, Opatija, Croatia.

IMPROVING SECURITY AND BATTERY POWER CONSERVATION IN WIRELESS SENSOR NETWORKS BY ALLEVIATING DOS ATTACKS

Dr. K. Srinivasulu[1]., A.Triveni [2]., A.Meena [3]., A Neha [4]., A.Vardhini [5].,

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

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Sensor nodes, which are the building blocks of sensor networks, are powered by battery resources, the lifespan of which is of great importance. Because sensors are used to monitor sensitive areas, security and energy efficiency are important factors when designing wireless sensor networks (WSNs). The sleep denial attack is a specific type of denial-of-service (DoS) attack that targets a battery-powered device and quickly depletes this limited resource. In order to achieve minimum energy consumption, sensor networks regularly switch the sensor nodes to standby mode. This is achieved through the use of MAC (Media Access Control) protocols. These protocols are designed to reduce the power consumption of the sensor nodes by keeping the antenna in standby mode as much as possible. This leads to energy savings. MAC protocols change the idle time depending on the type of communication required. However, malicious nodes can be introduced into the network. These attackers use your information in the MAC protocol to change the idle time of the node and thus shorten the life of the node. This document explains the sleep denial attack on WSN while proposing a scheme to authenticate new nodes attempting to change the nodes' sleep schedule. Only transmissions from valid nodes are accepted. The document provides detailed analysis for various scenarios and also explains the performance in implementing this secure authentication

Keywords— sensors, denial-of-service, denial-of-sleep, power failure, MAC protocol (Media Access Control)..

1. INTRODUCTION

Wireless sensor networks (WSNs) can be used to monitor environments and therefore offer a variety of interesting applications. Applications that can use WSN may be sensitive in nature and therefore may require an enhanced secure environment. The sensor nodes are operated with batteries. Since sensor nodes are used in harsh environments, they cannot be charged. Because of the unattended provisioning and the inability to charge, the power consumption of the node must be optimal. Many programs are offered to extend service life, save energy, and ensure safety in WSN. The duty cycle approach [1] is one of the systems with which energy can be saved better and more efficiently. During the duty cycle, nodes are periodically woken up to recognize the preamble from sleep mode to active, active to inactive, inactive to sleep mode.

The sleep denial attack is one of the low-energy attacks that tries to keep the sensor nodes awake in order to use more energy from the restricted power supply. It is difficult to replace sensors that fail due to battery discharge, and an anti-node without a safety mechanism can often transmit an incorrect preamble. If the receiver cannot tell the difference between the real and the false preamble, the receiver receives and processes the data from the anti-node. Such an attack keeps the receiver awake as long as the data transmission is maintained, which quickly drains the node battery.

The node's battery drains repeatedly and rapidly. In order to extend the service life of the individual sensor nodes and thus the entire sensor network, the battery charge carried by these nodes must therefore be retained. Therefore, the sender and recipient need mutual authentication schemes in order to counteract such attacks. If we cannot stop the attack, the life of the network can be shortened by months, even years, or even days. To avoid this attack, we need to authenticate the nodes, which changes the idle time of the nodes so that only synchronization messages from authenticated nodes are accepted.

Wireless sensor networks prefer the symmetrical algorithm to avoid the complicated calculations and high power consumption shown in Figure 1. However, encrypted data further exacerbates battery drain during a sleep-denial attack. The anti-node can send the "falsified" encrypted data to the recipient. This attack forces the recipient to decrypt the data. Before the receiver realizes that the data is "forged", the receiver uses more power to receive and decrypt the data.

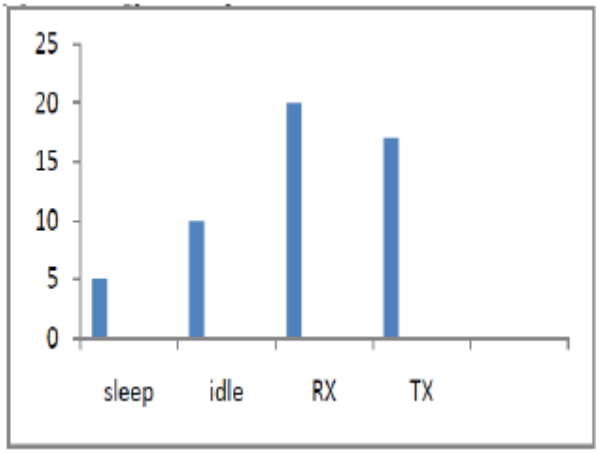


Figure 1. Electricity consumption

2. EXISTING SYSTEM:

B-MAC and X-MAC are LPL-MAC protocols (Low Power Listen-In) initiated by the sender, in which the receiver is triggered regularly in order to recognize the sender's preamble and then to receive and process the data.

2.1. B-MAC

The sender sends the long preamble as long as there is data to be sent to cover the embargo period and ensure that the recipient is active and recognizing. Since the B-MAC protocol does not have an ACK, the recipient has to listen and wait for the sender's long preamble to end. This long preamble concept consumes a lot of energy from both the sender and the receiver. Figure 2 shows the chronology of the protocol.

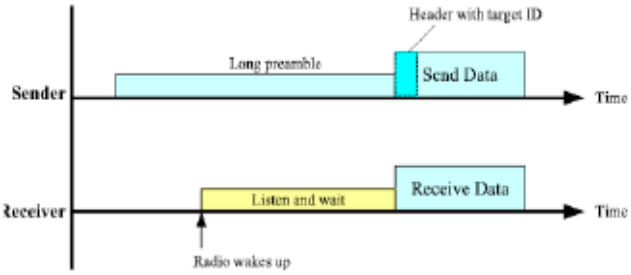


Figure 2. Chronology of the B-MAC protocol

2.2. X-MAC

When the sensor node has packets to send to the master node, it repeatedly sends the small preambles for a maximum duty cycle period. When the primary node wakes up, it receives the preamble and sends an acknowledgment packet [4]. After receiving the confirmation, the sensor node knows that one of the preambles has successfully reached the master node and then sends the data packet. Figure 3. shows the chronology of the X-MAC protocol. The primary node goes to sleep again if it does not listen to any data packet intended for itself for the duration of the wake-up period. If additional data needs to be sent to the master node, the sensor node immediately tries to transfer the data as well. Although there is no sender and the primary node does not listen to any data packets intended for itself in wake-up mode, the primary node is simply put back into the idle state after the wake-up period. 'At the next polling interval. Note that if the shipper is unable to deliver the package for a duty cycle period, they will stop and report FAIL to the user agent.

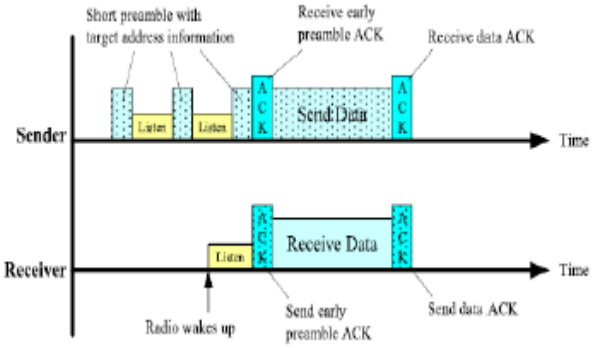


Figure 3. Chronology of the X-MAC protocol.

3. PROPOSED SYSTEM

3.1. RI-MAC

In Ri-MAC, the main node sends a beacon that notifies its sensor nodes that it is ready to receive data packets when it wakes up. The beacon carries the maximum recoil value tmax. When the sensor node that has data to send receives the beacon, it first selects a random return time t between 0 and tmax ms. The sensor node then waits for this random duration (tms). After tms, the sensor node sends the outstanding data packet. When the data packet is received, the head node sends a confirmation packet that contains the sequence number of the data packet and also tmax. The sequence number in the confirmation packet informs the sensor node of the successful delivery, and the sensor node stays awake until it hears a confirmation from the receiving node. The primary node beacon initiates data transfers. T

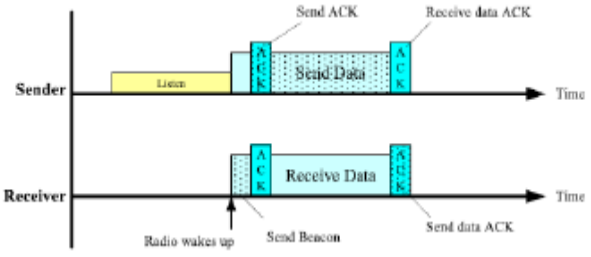


Figure 4. Chronology of the X-MAC protocol.

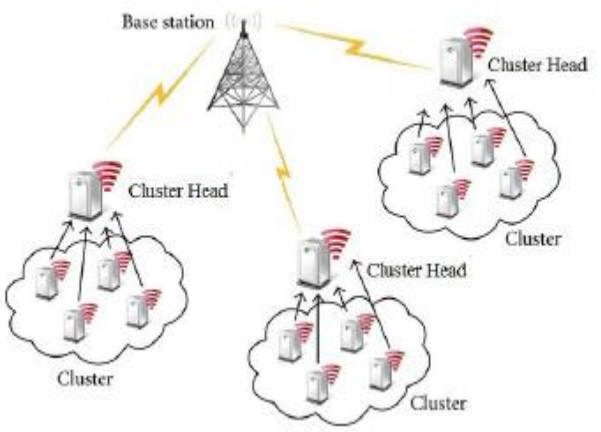


Figure 5: System Architecture

he sensor node goes to sleep when there are no more data packets. Figure 4 shows the chronology of the RI-MAC protocol. The tmax in the confirmation packet is used to initiate a new data transmission. If the primary node does not receive any incoming data packets before tmax has expired, it is put back into the idle state until the next scheduled wake-up time. If there are multiple senders, package collisions can occur. For example, S1 and S2 want to send packets to the master node, but they randomly select timer shutdown times. If the primary node detects a packet collision on the channel, it sends a new beacon with a higher tmax after the previous tmax has expired. With a higher tmax for the next period, Ri-MAC would like to increase the probability that more than one sender will select retracement times further away. Note that if the shipper cannot deliver the package within one duty cycle, they will stop and report FAIL to the user agent.

4 RESULT

These processes also keep sensor nodes awake longer. The integration into the MAC protocol requires a fast and simple mutual authentication scheme in order to counter attacks with "forged" encrypted data. This document proposes a layered secure scheme design that includes the Two-Tier Energy Efficiency Secure Scheme (TE2S) MAC protocol to protect WSNs from previous attacks. The aim of the design is to simplify the security process against attacks with low power consumption. This scheme uses the hash string to generate the dynamic session key, which can be used for mutual authentication and symmetric encryption key. The only dynamic session key computations are hash functions, which are quick and easy. This scheme can counteract replay and spoofing attacks and also shows that this scheme is also energy efficient [3].

5 CONCLUSION:

Security and energy efficiency are top concerns when designing wireless sensor networks (WSN) because they are susceptible to various types of intrusions and attacks on the network. The rationale of the project is to identify the malicious node and collect the details of the attacker. The MAC protocol tries to reduce the power consumption of sensor nodes by keeping the antenna in standby mode. The proposed method provides strong authentication that defends the denial of the attack that has been paused and activates the defense mechanism only in the attack zone where the firewalls prevent the attacker from performing the task. The above diagram is effective on the home page of the sender and the home page of the recipient. The proposed system can defend against attacks such as tampering with attacks, repetition of attacks, and put sensor nodes back to sleep as soon as possible to save power.

REFERENCE

1. Mechanisms for Detecting and Preventing Denial of Sleep Attacks and Strengthening Signals in Wireless Sensor Networks Chandrakala. P. Goudar1, Shubhada. S. Kulkarni2 1P G Student, Gogte Institute of Technology, Belagavi, Karnataka, India 2Asst Prof, Dept of C S E, Gogte Institute of Technology, Belagavi, Karnataka, India
2. "A Secure Scheme for Power Exhausting Attacks in Wireless Sensor Networks" Ching-Tsung Hsueh, Chih-Yu Wen and Yen-Chieh Ouyang Department of Electrical Engineering & Graduate Institute of Communication Engineering National Chung Hsing University Taichung, Taiwan 40227
3. "Tees-Two-Tier Energy Efficient Secure Scheme For Increased Network Performance In Wireless Sensor Networks", Veena M kanthi. IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India
4. CS 450: Homework 3 ,Implementation and Comparison of X-MAC and Ri-MAC

DETECTION AND RECOGNITION OF TRAFFIC SIGN USING MACHINE LEARNING AND OPEN CV

P.Manju [1] .,Ch.Haritha [2]., Ch.Saisri [3]., Ch.Harika [4] ., D.Prathiba [5].,

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

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— This article describes the method of recognizing and recognizing traffic signs. In the learning-based recognition section, we review the Viola Jones detector and the ability to apply it to traffic sign recognition. The recognition of the recognized traffic sign is handled by the SVM classifier based on the gradient histogram. Overall, this system is expected to perform much better than the other systems available. It has been shown that algorithms, when trained with the right images, work precisely. This should also apply to road signs of different colors, lighting and weather conditions.

Keywords* : *OpenCV, hair features, cascade classification, machine learning, gradient histogram, cascade training, SVM, ANN, feature matching.

1. INTRODUCTION

In recent years, the computing power that has made computer vision possible for consumer applications has increased. As computers offer ever more computing power, the goal of recognizing and recognizing traffic signs in real time is becoming achievable. Some newer models of premium vehicles are already equipped with driver assistance systems that enable automatic recognition and recognition of certain classes of traffic signs. The recognition and recognition of traffic signs is also of interest in automated road maintenance.Traffic symbols have several distinctive features that can be used for recognition and identification. They are designed in specific colors and shapes, with the text or symbol contrasting with the background. Every route should be checked regularly for missing or damaged signs. as such, signs pose a security threat. Checks are typically performed by driving a car on the road of interest and manually recording any problems observed. Manually checking the condition of each traffic sign is tedious, tedious, and prone to human error. By using computer vision techniques, the task could be automated and therefore carried out more frequently, which leads to increased traffic safety.

2. RELATED WORKS

Most systems use color information as a method of segmenting images. Color-based traffic sign recognition performance is often degraded in scenes with strong lighting, poor lighting, or adverse weather conditions such as fog. Color models such as HSV (Hue Saturation Value), YUV and CIECAM97 have been used to overcome these problems. For example, Shadeed et al. Segmentation performed by applying the U and V chrominance channels of YUV space, where U-positive and V-negative for red colors. This information was used in combination with the hue channel of the HSV color space to segment the red traffic signs.

Gao et al. applied a four-tree histogram method to segment the image based on the hue and chroma values of the CIECAM97 color model. Malik et al. Set the threshold for the HSV color space tone channel so that red traffic signs are segmented. In contrast, there are several approaches in which color information is completely ignored and only the shape information of grayscale images is used instead. For example, Loy and Zelinksy proposed a system that uses local radial symmetry to highlight points of interest in each image and identify octagonal, square, and triangular road signs. Some newer methods like and use HOG functions to extract traffic sign functions. Creusen et al. extended the HOG algorithm to include color information using CIELAB and YCbCr color spaces.

Overett et al. presented two different formulations of the HOG functionality for speed sign recognition in New Zealand. We also use the HOG functions to simplify our ranking process and will explain later why we found them best for this application. The vast majority of existing systems consist of classifiers trained on hand-lettered images. This is a repetitive, time-consuming, and error-prone process. Our method avoids the

manual collection and labeling of training data, as only synthetic graphic representations of the signs are required, which have been retrieved from an online traffic sign database. Although many existing systems report high classification rates, the total number of traffic sign classes recognized is generally very limited and therefore less likely to be missing similar characters from their databases.

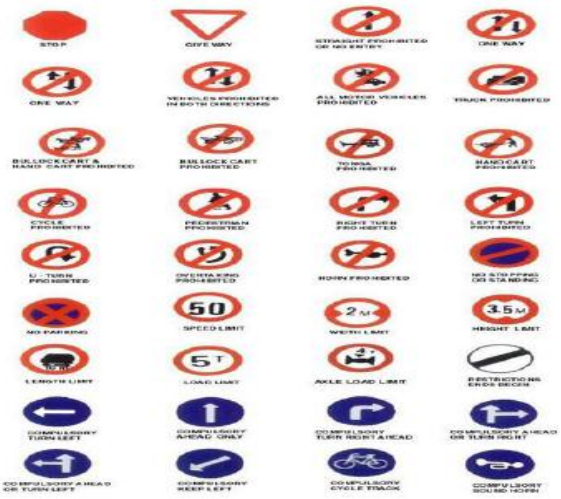


Fig. 1. Some examples of road signs.

If our system made an error of 1 false positive out of 10 frames, there would still be 8,560 false positives or two false positives per second left in one hour, rendering the system completely unusable for any serious application. To further complicate the problem, the vehicle in which a commercial traffic sign recognition system is implemented cannot be expected to be equipped with a very high definition camera or other useful sensors, since the addition of such sensors increases the production cost.

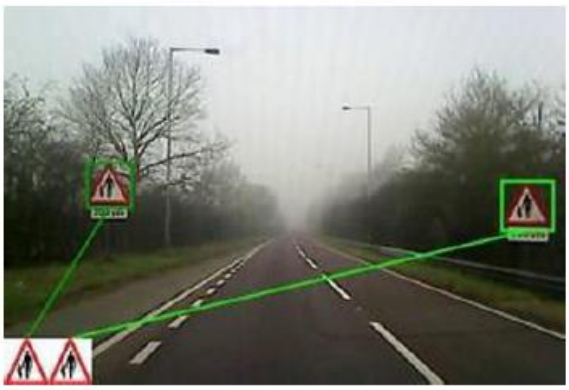


Fig. 2: Example of an ideal traffic sign recognition system

3. PROPOSED SYSTEM

Our proposed system uses all instances of ideogram-based traffic symbols and therefore compares them to this larger set. We hope that our approach will also work when applied to databases of traffic signs from other countries that have been accessed in the same way. It should be noted that many of the proposed systems suffer from slow speed, which makes them unsuitable for application to real-time problems.

3.1 Detection And Recognition Of Traffic Signals

The proposed system comprises the following two main stages: detection and detection. The full set of road signs used in our training data and recognized by the system. The system uses Raspberry Pi as the processing module and OpenCV as the software module.

The detection stage uses hair cascades based on the hair properties of an object to identify a traffic sign. It is a machine learning based approach in which a cascade function is formed from many positive and negative images. It is then used to identify objects in other images. Initially, the algorithm needs many positive images (signed images) and negative images (unsigned images) to train the classifier. So we have to extract the functionality from it. For this purpose, the properties of the hair shown in the picture below are used. They are like our convolution core. Each feature is a single value obtained by subtracting the sum of the pixels under the white rectangle from the sum of the pixels under the black rectangle. Now all possible sizes and positions of each kernel are used to compute many features. (Imagine how many calculations do you need?

Even a 24x24 window offers more than 160,000 functions. To calculate each feature, we need to find the sum of the pixels under the black and white rectangles. The first feature chosen seems to focus on the property that the drawing area is generally darker than the inner area. All the required functions are written to the file, which is then loaded during runtime. The recognizing step makes it possible to confirm a candidate region as a road sign and to classify the exact type of sign. To classify candidate regions, their HOG

properties are extracted from the image, which represent them the appearance of the gradient orientations in the image.

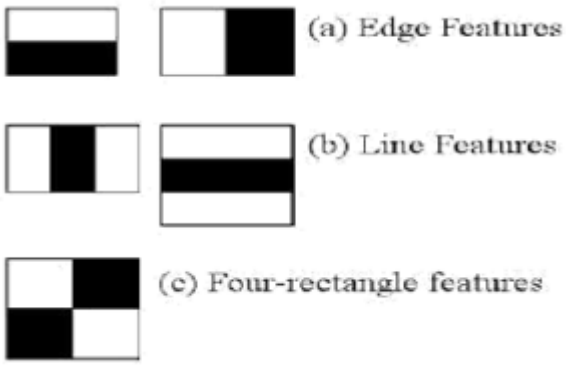


Fig. 3. Desired properties in an image.

HOG feature vectors are calculated for each candidate region. A Sobel filter is used to find the horizontal and vertical derivatives, and therefore the size and orientation of each pixel. We think the application of HOG is very well suited for recognizing traffic symbols, as the traffic symbols consist of strong geometric shapes and high-contrast edges that cover a range of orientations. Road signs are generally approximately straight and point towards the camera, which limits rotational and geometric distortions and eliminates the need for rotational invariance. The HOG properties are calculated in a dense grid of cells using local contrast normalization in overlapping blocks. A histogram of nine size-weighted unsigned pixel orientation groups is created for each cell. These histograms are normalized in each overlapping block. The components of the feature vector are the histogram values for each normalized cell.

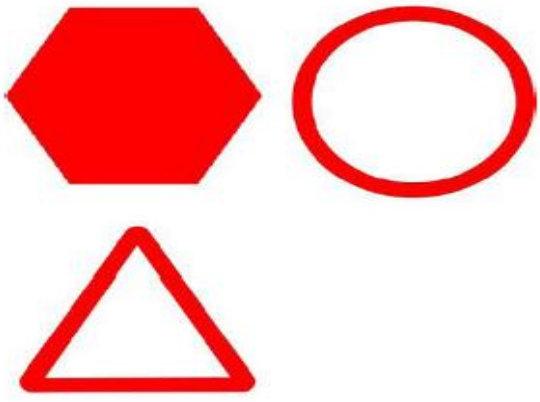


Fig. 4. Examples of images used to train the waterfall

The regions are then classified using a multiple class SVM cascade. SVM is a supervised learning method that creates a hyperplane to divide data into classes. "Support vectors" are data points that define the maximum edge of the hyperplane. Although SVM is primarily a binary classifier, classification of multiple classes can be achieved by training many binary SVMs individually. SVM classification is fast, very accurate and, compared to many other classification methods, less prone to overvoting. It is also possible to train an SVM classifier very quickly, which is very helpful with the method we proposed given our large amount of training data and the large number of classes. However, we plan to make further comparisons with other classification methods in future work. Each region of our system is classified using a cascade of SVM classifiers. First, the size of the candidate area is changed to 24 × 24 pixels. A 144-dimension HOG feature vector is then calculated and this feature vector is used to classify the shape of the region as a circle, triangle, inverted triangle, rectangle, or background. Octagonal stop signs are seen as circles. If the region is in the background, it will be rejected. If the range is found to be a shape, it is passed to a subclassifier (symbol) for that particular shape.

4 RESULT AND DISCUSSION

The system uses the Viola-Jones algorithm to recognize the characters. This is a very fast and accurate algorithm when trained properly. This enables detection on all integrated peripheral devices when the available computing power is low. In addition, the system uses the HOG algorithm to extract functions for training the SVM cascade, which in turn is very precise. The extracted features are then sent to the SVM cascade instead of other algorithms like ANN, KNN that are not as accurate as the SVM algorithm. In addition, SVM does not have a K value like ANN, which slows it down as the value increases.

5 CONCLUSION

We have proposed a new real-time system for the automatic detection and recognition of traffic symbols. Candidate regions are recognized as hair waterfalls. This detection method is very insensitive to changes in lighting and lighting conditions. Traffic symbols are recognized by HOG functions and

a cascade of linear SVM classifiers. A method for the synthetic generation of training data has been proposed with which large data sets can be generated from model images without the need for manually labeled data sets.

REFERENCES

1. Sergio Escalera and Petia Radeva, "Fast greyscale road sign model matching and recognition", Centre de Visióper Computador Edifici O – Campus UAB, 08193 Bellaterra, Barcelona, Catalonia, Spain.
2. W. Shadeed, D. Abu-Al-Nadi, and M. Mismar, "Road traffic sign detection in color images," in Proc. ICECS, 2003, vol. 2, pp. 890–893.
3. X. Gao, L. Podladchikova, D. Shaposhnikov, K. Hong, and N. Shevtsova, "Recognition of traffic signs based on their color and shape features extracted using human vision models," J. Vis. Commun. Imag. Represent., vol. 17, no. 4, pp. 675–685, Aug. 2006.
4. Gary Bradski and Adrian Kaehler, "Learning OpenCV", 1st Edition, O'Reilly Publications, pages 459-521, 2008.
5. Jack Greenhalgh and Majid Mirmehdi, "Real-Time Detection and Recognition of Road Traffic Signs", IEEE Transactions on Intelligent Transportation Systems, Vol. 13, No. 4, pages 1498-1506, December 2012.
6. Auranuch Lorsakul1 and Jackrit Suthakorn, "Traffic Sign Recognition Using Neural Network on OpenCV: Toward Intelligent Vehicle/Driver Assistance System".
7. R. Malik, J. Khurshid, and S. Ahmad, "Road sign detection and recognition using color segmentation, shape analysis and template matching," in Proc. ICMLC, Aug. 2007, vol. 6, pp. 3556–3560.

DETECTION OF DISEASES IN LEAVES USING K-MEAN CLUSTERING AND FEATURE EXTRACTION USING GLCM

Swetha, B[1] ., D.Swetha [2]., D.Swetha [3]., D.Sushmitha [4] ., D.Vinitha [5].,

1 Assistant Professor, Department of ECE., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ bswethaece@mrcew.ac.in)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Agricultural products are susceptible to disease as they are attacked by fungi and bacteria and are also affected by poor environmental conditions. Symptoms are first visible on leaves, stems, etc. This article suggests a method for detecting leaf diseases. The aim is to identify and classify diseases. Sheet images are taken and some are used for training purposes, others as test images. The proposed method first improves the image, then converts the RGB image to an HSV color space and then segments the diseased part from the healthy part by K-mean clustering. Feature extraction is done by GLCM and classification is done by SVM.

Keywords : coexistence matrix; SVM; Texture characteristic; Grouping of k-means..

1. INTRODUCTION

India is an agricultural country. The economy depends mainly on agricultural products. The main goal is to increase the economy by increasing production and improving the quality of fruits and vegetables. Today, due to the environmental conditions, the quality of agricultural products is deteriorating as they become susceptible to various diseases. That is why it is necessary to identify diseases as early as possible. The first symptoms appear on the leaves first. Therefore, by recognizing diseases early, treatment can be carried out early and thus increase the yield and also improve the quality of the fruit.
Manual disease inspection in a very large field is a very long process and farmers cannot manage more than one farm. So there needs to be a system that automatically detects diseases and then only the processing is provided. The easiest way is to use image processing techniques.

2.ANALYSIS OF PLANT DISEASES

The proposed work focuses on strawberry leaves.
Leaf spot is caused by Mycosphaerella fragariae. There are small round purple to reddish spots on the top of the leaves. The centers of these spots are gray to white.

Fig 1 Leaf spot
Burned leaf
Leaf rot is caused by Diplocarpon earliana. In this disease, the spots have 2 forms; large or small numbers of small point points and / or points with points 1/4 to 1/2 inch in diameter. The burn marks are usually reddish brown in color.

Fig 2Burned leaf
Leaf rot is caused by Phomopsis obscurans. There are red-purple spots with brown centers.

Fig 3 Leaf rot

3. LITERATURE REVIEW

The methodology proposed in [1] shows that the image preprocessing is carried out in order to eliminate noise such as Gaussian noise, salt and pepper noise. Then segmentation is done by grouping the k-means. Then the properties

are extracted by GLCM and the classification is carried out by ANN.
In [2] the properties of color, morphology and texture are extracted instead of simple properties of the texture. The classification is carried out by ANN.
In [3] the color and texture features are extracted using a histogram and comparing the pixel values with neighboring pixels. The classification is carried out by ANN.
In [4] the color and texture features are combined, then the classification is carried out using the random forest classifier.

4. PROPOSED METHODOLOGY

There are five main steps in the detection of plant leaf diseases as shown in FIG. The proposed method comprises the following steps: input image, image preprocessing, segmentation, feature extraction and classification.
A. Image acquisition:
This is the basic and basic step as the processing of the images is done.
B. Image preprocessing:
Image preprocessing consists of two tasks: image enhancement and color space conversion. The RGB image is converted to an HSV image.

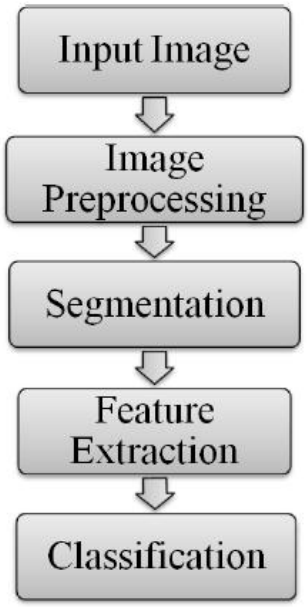


Fig 4 Block Diagram of Proposed Methodology

C. Image enhancement:
The image is enhanced by balancing the histogram. This is done to improve the contrast of the image. The histogram equalization is performed on a grayscale image. The image is then converted into RGB format and then into YCbCr format.
D. Color space conversion
This plays an important role in the detection of leaf diseases. The RGB images of the strawberry leaf are converted to HSV. The hue describes the purity of the color that a viewer perceives. The saturation refers to the amount of white color.
Image segmentation:
Image segmentation is used to separate the diseased part from the healthy part. The grouping of the mean value K with the value K = 4 is used here.

5 RESULTS

Fig 5 Original image

Fig 6 Histogram Equalized image

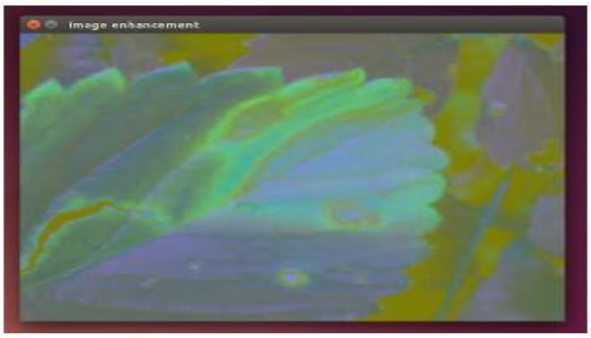


Fig 7 Enhanced Image

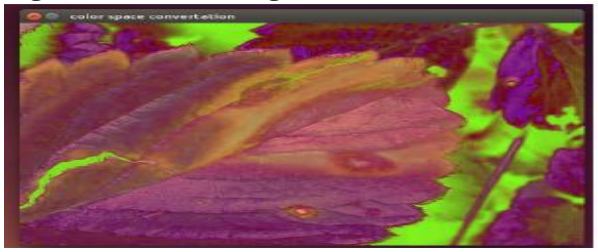


Fig 8 HSV picture

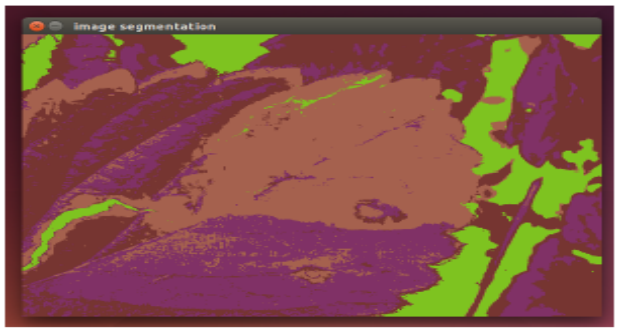


Fig 9 Segmented image

5. Conclusion

The classification with SVM is more accurate if there are fewer training images. ANN is complex compared to SVM. Once ANN is formed, changes are difficult as it behaves like a black box. ANN is the neural network in which the neurons are the extracted features. There are hidden layers in ANN that make editing difficult. Making changes is easier in SVM than in ANN. ANN and Random Forest Classifier require a large number of training images compared to SVM. SVM resists distortions in training images.

REFERENCES

1. Mrunmayee Dhakate and Ingole A. B. "Diagnosis of Pomegranate Plant Diseases using Neural Network" IEEE.
2. Ashwini Awate, Damini Deshmankar, Gayatri Amrutkar, Utkarsha Bagul, Prof. Samadhan Sonavane "Fruit Disease Detection using Color, Texture Analysis and ANN" 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).
3. Bhavini J. Samajpati and Sheshang D. Degadwala "Hybrid Approach for Apple Fruit Diseases Detection and Classification Using Random Forest Classifier" International Conference on Communication and Signal Processing, April 6-8, 2016, India.
4. Jun Lu, Pengfei Wu, Jiwei Xue "Detecting Defects on Citrus Surface Based on Circularity Threshold Segmentation" 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).
5. Monika Jhuria, Rushikesh Borse "Image Processing for Smart Farming: Detection of Disease and fruit grading" 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).
6. Sudhir Rao Rupanagudi, Ranjani B.S., Prathik, Nagaraj ,Varsha G. Bhat "A Cost Effective Tomato Maturity Grading System using Image Processing for Farmers" International Conference on Contemporary Computing and Information,2014.
7. Pradnya Ravindra Narvekar, Mahesh Manik Kumbhar2, S. N. Patil "Grape Leaf Diseases Detection & Analysis using SGDM Matrix Method" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3237:2007 certified organization) Vol.2,Issue 3, March 2014.

NEURAL NETWORK BASED VOICE CLASSIFICATION USING EGG AND MFCC FEATURE

S. Prabhakara Rao[1]

Professor, Department of ECE., J B R Engineering College., Moinabad., TS, India,
(✉ prabhakararao_ece99@gmail.com)

2, 3, 4, 5 B.Tech IV Year ECE, (17RG1A0459, 17RG1A0445, 17RG1A0429, 17RG1A0440), Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract*— Speech recognition is a subjective phenomenon. This method still faces a significant problem. Different techniques are used for different purposes. In this project we show how speech signals are perceived in the neural system using the FCM (c-implicate fuzzy clustering) method. The voices of different people of different ages are recorded in silent and silent conditions with a high quality receiver. These people speak the same sentence of the term for 10-12 seconds. These spoken sentences are then switched to wave positions. At this time, the components of the recorded examples are erased by preparing these signals using LPC. These systems are ready for use thanks to pattern recognition. Their significance for the sequence and presentation of compound content is insignificant; Regardless, most viable speech recognition frameworks rely heavily on speech recognition to reach the elite. To classify vowels using an adaptive median filter with a combination of EGG and speech information. The Mel frequency cepstral coefficients (MFCC) and the neural network (NN) are used as components that represent the speech signal.

Keywords* : *adaptive median filter, FCM grouping method, MFCC, neural network, speech recognition, learning algorithm..

1. INTRODUCTION

Speech recognition systems in particular for testing the accuracy of the speech signal. The speaker's emotional state can make all the difference in how different people pronounce. The environment can add noise to the signal. Sometimes the speaker itself causes the noise to expand. Speech recognition changes the voice signal picked up by the microphone or phone to a character layout. Therefore, humans could use language as a valuable interface when interacting with machines. Humans need to reliably achieve a distinctive, possessive, and synchronous representation of speech recognition performance. The work as a powerful classifier for vowels with stationary spectra of these systems has been successful. To promote the further development of the multilayered neural system is not prepared to process different temporal data such as spectra of speech sounds that change over time.

2. WORD RECOGNITION OF THE WORD AND EI DATA COMBINATION

In general, almost all speech recognition (SR) systems involve the following steps: signal preprocessing, feature extraction, and classification. Speech recognition is used by two different training and testing methods.

2.1. Signal preprocessing

In an environment where noise is not available, a different sound will be picked up by a microphone. These speech signals are classified in many other ways for speech recognition such as those used by preprocessing, filtering, and mel-frequency cestrum coefficients. The samples are recorded with a microphone. First, low and high frequency noise is removed by digital filtering. Speech signals are mainly between 300 Hz and 750 Hz. Preprocessing units can be used to identify signals in the time domain prior to feature extraction.

Typically, in the preprocessing step, the speech signal is used for analog-to-digital (A / D) conversion, enhancement and filtering, and generally to remove silence from the SR application.

2.2. Feature extraction

It extracts some important information from the voice signal. Feature extraction can be viewed as extracting certain mathematically parameterized information from the original source signal. There are many feature extraction techniques that can be used. The example includes Fast Fourier Transform Coefficients (FFT) and Mel-Cepstral Frequency Coefficients (MFCC). In this study we decided to use MFCC as functionality.

2.3. EGG signal and speech classification.

The input language or the test signal for determining the input language supplied corresponds to the desired target language. Some of the categories of classification schemes are speech and non-speech sections that use the neural network (NN) approach.

3. PROPOSED METHODOLOGY

In this article, frame segmentation is generally used to break down the speech signal. This is not enough for short and voiceless consonants. The combination of EGG information and voice signal is used. EGG provides information about the vibration of the vocal cords. A median filter is used in the preprocessing phase. This combination of EGG information and voice data is used for the input signal. In the preprocessing step, envelope detection and the adaptive median filter can be used to remove noise. Thus, when different temporal alignments of the vocal segment are detected, it creates a section of vowels and consonants. The segmentation of speech sections and the recognition of unvoiced consonants are combined into phonemes using a neural network.The classification of the speech signal is a very important phenomenon in speech recognition.

The neural network is used for preprocessing, recognizing and classifying the envelopes of various speech signals. A number of processing units used to process the speech signal.The combination of speech and EGG data is defined as a waveform that is created when the vocal cords vibrate. The adaptive median filter is used to remove noise and classify vocal and non-vocal sounds.

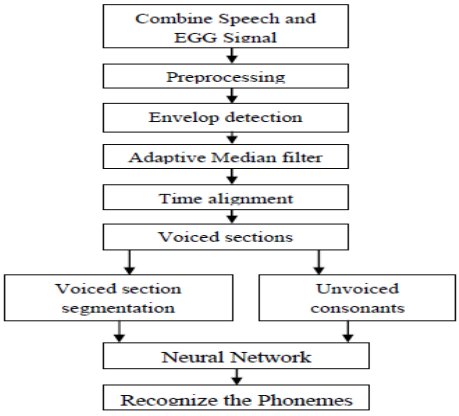


Fig. -1: Flow chart of the proposed method

Very simple techniques like preprocessing, filtering are handled by these types of units.

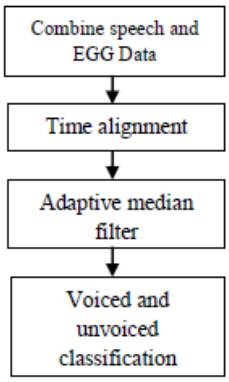


Fig. 2: Flow diagram for the detection of sound sections

They improve the success rate (HR), the signal-to-noise ratio (SNR) and reduce the false alarm rate (FA). Follow this equation like:

$$SNR = \log_{10}\left(\frac{\mu}{\sigma}\right)^2 \ldots\ldots\ldots\ldots (1)$$

Where

μ = mean and σ = standard deviation .

$$HR = \frac{NH}{NR} \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Where NT is the total number of limit values recognized, NH is the number of correctly recognized limit values and NR is the total number of limit values.

$$FA = \frac{NT-NH}{NT} \ldots\ldots\ldots\ldots\ldots (3)$$

In order to be able to assess the overall quality of a segmentation method, an overall measure is required which takes these assessments into account at the same time. A well-known measure is the value F1 in the form of an equation:

$$F1 = \frac{2\times(1-FA)\times HR}{(1-FA)+HR} \ldots\ldots\ldots (4)$$

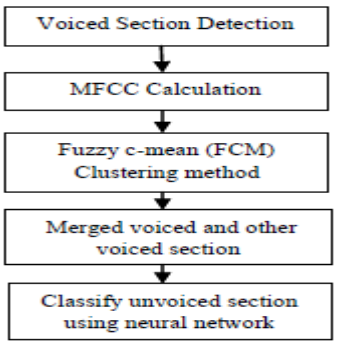


Fig. -3: Flow diagram of the segmentation of the sound section

The vowel section consists of more than one vowel, semi-vowel, or consonant. It has been shown that the cepstral frequency coefficient Mel (MFCC), the speech data in each tone cycle has a fixed length. The FCM grouping method to avoid spectrum loss. Merging by Sounds and other sections are covered separately. As such, it is classified into the unvoiced portion using the neural network.

The MFCC calculation contains the speech data in each tone cycle and is terminated with trailing zeros up to a fixed length n (128 is selected). The hammer window is used to prevent the spectrum from leaking. The quadratic amplitude discrete Fourier transform (DFT) converts the windowed speech data into the frequency domain so that the short-term power spectrum P (f) is obtained. The spectrum P (f) is then filtered through a group of triangular band pass filters along the frequency axis Mel. The output is a set of subband energies E (d), d = 1,2, … D. The MFCC is calculated using the logarithm of Equation E (d) as follows:

$$C(i) = \sqrt{\frac{2}{D}} \sum_{d=1}^{D} [\log(E(d)) . \cos \frac{(2d-1)i\pi}{2D}] \ldots\ldots (5)$$ Where i = 1 … D.

The Viterbi algorithm aims to find the optimal segment state sequence in order to realize the reassignment of a sequence to several groups.

4. RESULTS AND DISCUSSION

The combination of voice signal and EGG is used as input in this project. A spectrogram is a visual representation of the frequency spectrum in a tone or other signal as it varies with time or some other variable. The Hilbert envelope is important for signal processing, where it derives the analytical representation of a signal. The adaptive median filter is used to remove noise. Finally, classify the vocal and non-vocal areas using the neural network.

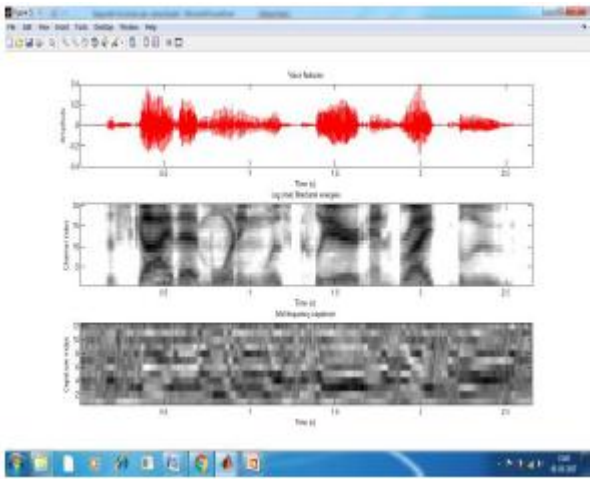


Fig. -4: Detection of the sound section

Figure 4 shows that the detection of the speech portion is speech using speech properties aligned with speech derivation and EGG.

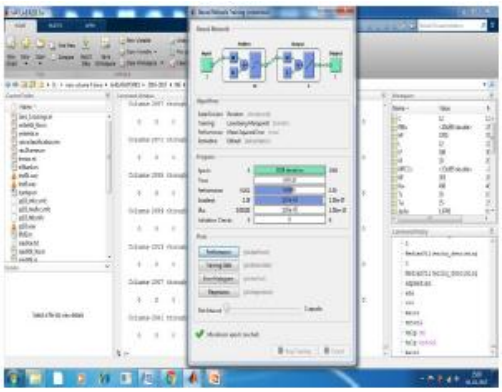


Fig. -5: Classification of neural networks

Figure 5 shows that the command is a neural network classification used by the network to process the records of the training set individually using weights and functions. They process the records one by one and learn by comparing their record ranking with the actually known ranking of the records.

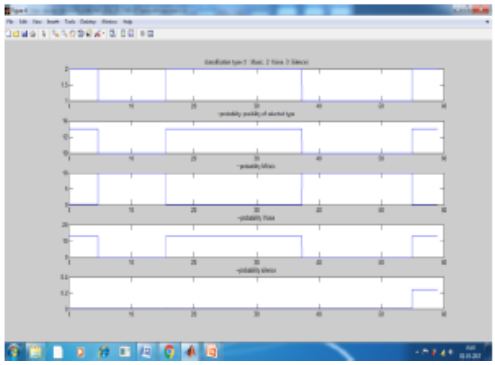


Fig. 6: Classification of the output signal

No of samples Signal	SNR Value	Accuracy Value
Test wave.1	1.73db	87.3%
Test wave.2	3.12db	90%
Test wave.3	6.23db	92%
Test wave.4	8.00db	96%

Table -1: SNR and accuracy value

Figure 6 shows that the utterance is a classification of the output signal for different types of music, speech, and silence. Each section is dealt with separately. The segmentation of the unvoiced section to classify the unvoiced section in the detection of the unvoiced section and the RMS calculation.

5. CONCLUSION

In this document, the maximum average accuracy for each network was 91.5%. EGG is used to develop an accurate and robust method for text-independent phoneme segmentation . Unlike traditional methods, phonemes are initially divided into two categories called vowel (including vowels, half-vowels, and some consonants) and voiceless (other consonants). There is a comparison with the most accurate SNR value and accuracy.

REFERENCES

1. Dr. R. L. K. Venkates, Dr. R. Vasantcha Kumari, G. Vani Jayasatu, “Speech Recognition using A Radial Basis Function Neural Networks” volume.3, PP 441-445, April 2011, 3rd INC on E computer technique IEEE.
2. Khanagha.V et al (2014), “Phonetic segmentation of speech signal using local singularity analysis,” Digital Signal Process., vol. 35, pp. 86–94.
3. Park, S.S., Shin, J.W., Kim, N.S., “Automatic Speech Segmentation with Multiple Statistical Models”, in Proceedings of Interspeech, 2006.
4. Wouter Geuaert, Georgi Tsenav, Valeri Mladenov, “Neural Network used for Speech Recognition” Journals Automatic Control, volume.20.1.7, 2010
5. K. Daqrouq, "Wavelet Entropy and Neural Network for Text-Independent Speaker Identification," Engineering Applications of Artificial Intelligence, vol. 24, pp. 796-802, 2011.
6. Amit.J and Carol.E.W (2003),“Speech segmentation using probabilistic phonetic feature hierarchy and support vector machines,” in Proc. Int. Joint Conf. Neural Newts., vol. 1, pp. 675–679.
7. S. Granqvist et al., “Simultaneous analysis of vocal fold vibration and transglottal airflow: Exploring a new experimental setup,” J. Voice, vol. 17, no. 3, pp. 319–330, 2003.
8. J. Neubauer et al., “Coherent structures of the near field flow in a selfoscillating physical model of the vocal folds,” J. Acoust. Soc. Amer., vol. 121, no. 2, pp. 1102–1118, 2007.

TCL SCRIPT GENERATOR WIRELESS NETWORK WITH NETWORK ANALYZER AND REPORT GENERATION USING NS-2

R.Mounika [1] ., A. Anil Kumar[2]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (: rmounika1@gmail.com)

2 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract: The network simulation tool is a solution for our complex generation of network scenarios. TCL (Tool Command Language) scripts are mainly used in the NS-2 simulation tool. The network simulation is used to create TCL scripts to configure wired or wireless network scenarios under NSG2.1 and then run those TCL scripts with the Network Simulation-2 tool to get the network with simulation results. The document focuses on the TCL script generator, how it was developed, how to save the TCL script, and how to run it with NS-2. I am going to introduce some unique functions of the "TCL Script Generator" with performance issues like performance, delay and jitter and would like to discuss different sound functions compared to NSG-2 (NS-2 Scenarios Generator2)

Keywords: TCL scripts; Network Simulator-2 (NS-2); NSG-2;Performance; Delay; Feel nervous.

1 INTRODUCTION

The network simulation provides the result of the network design, but it raises many questions about the network standards and the various material manufacturers that have an efficiency of the future network design model. Many designers use specialized software to solve network problems or queries. However, simulating communication networks is the most powerful and successful method for developing network productivity in network design. There are many simulation software available in the market today. All types of simulators have the same capabilities with some changes to the app language for UI, user design, user role, etc.Network simulation is the best evaluation method in the field of communication networks. This is particularly useful for improving the building of new communication designs and the design of network protocols. The NS-2 network simulator is the most widely used open source discrete event simulator. It is the most useful, scalable and efficient design tool for network simulation in design research for research and use of communication networks.

2. SIMULATION MODEL

Our evaluations of network scenarios are based on simulations with NS-2. NS-2 is a discrete event simulator that simulates a variety of IP network topologies. First, however, the simulation in existing systems with NSG2 is used. With the help of this simulation, the result of the proposed system is also obtained by analyzing the performance of the network.

A. Simulation environment

The simulation environment consists of wired or wireless nodes that form an ad hoc network. Simulation is one of the most important technologies of the advanced age. Computer aliveness can model speculative objects and actual activity on a computer, which enables them to be explored. The network is simulated on the computer. A network simulator is a technique for implementing a network against the computer. In this section we describe performance metrics and implementation details for network topologies. The performance of a system must be assessed according to certain criteria. These criteria then determine the basis for a system's performance. These parameters are known as performance metrics. The following performance metrics are considered when evaluating network topologies:

1) Power: This is the amount of traffic a network can carry.

2) Delay: This is defined as the time it takes for the package to be delivered to its destination. The delay should be as short as possible.

3) Jitter: This is defined as the variation in the delay of the packets belonging to the same flow.

B. Levels of simulation

Write a Tool Command Language (TCL) script and simulate the script with NS2 to analyze the specified problem. To use NS2, a user programs in the Object Tool (OTcl) command language. An OTcl script does the following steps.

• Start an event planner.

• Configure the network topology using network objects.
• Indicates to the traffic sources when to start / stop packet transmission via the event scheduler.

C. Implementation

The main simulation and network configuration on NS2 is done in the TCL script. After the network NS2 is described using the TCL script, it is executed and the output files are analyzed for the results. There are two main output files, a trace file with all events such as sending, receiving, deleting packets etc. and a NAM file which can then be used by the network animator to display the simulation in graphics mode.

B. Structure of the generic NS2 script

1. Create a simulator object
2. [Activate tracking]
3. Create a topology
4. [Settings for packet loss, connection dynamics]
5. Create routing agents
6. Create applications or traffic sources.
7. Post-processing procedure (i.e. NAM)
8. Start the simulation

3. PROPOSED SYSTEM

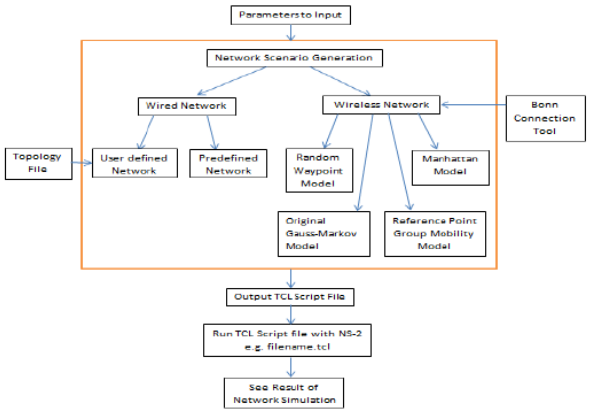


Figure 1: Event flow for a TCL file

In the proposed system, I have developed a new TCL script generator tool called 'ARGT for NS2' that allows authorized users to generate TCL (Tool Command Language) script files directly and flexibly. It has a graphical user interface (GUI). This tool has a very easy-to-use interface that allows you to set network restrictions on the design of wired and wireless communications. After entering the parameters or restrictions, the tool repeatedly creates a TCL script file that can be executed in the atmosphere of the communication network. NS-2 awards the network simulation output as a simulation for the examined network code scenarios. The program was developed using the Java language (Java Swings) to be compatible with different operating systems as it is platform independent. The authors have not implemented the Trace Analyzer. After reading the author's article and understanding the basics of network communication and the trace analyzer, I implemented network simulation reports and the design of the trace analyzer.

4. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

The requirements for environmental development are:

ARGT provided a standard toolbar in the GUI through which we can add nodes, connect any number of nodes via links (simplex / duplex) and define which protocols to use for communication by adding agents and finally adding applications that perform communication between nodes. The ARGT tool offers customizable log functions as well as customizable agents.

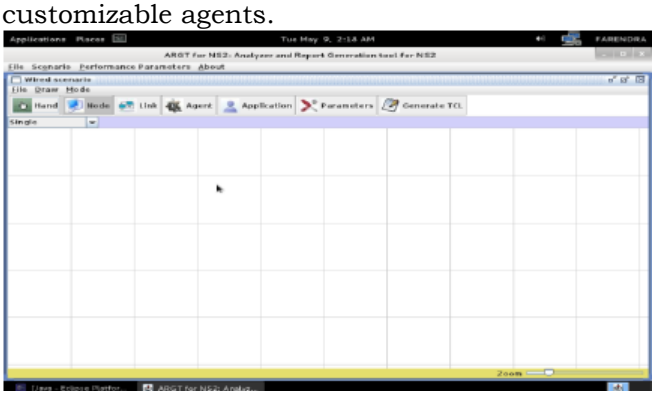


Figure 2 Main window with scenario grid

The user can add many nodes when creating the scenario. Given the wired scenario, the nodes can be connected by links. Simplex or duplex. Different protocols like TCP / Sink, TCP / Newreno, UDP etc. have been added. and applications such as the File Transfer Protocol (FTP) application and Constant Bit Rate (CBR) application have been added.

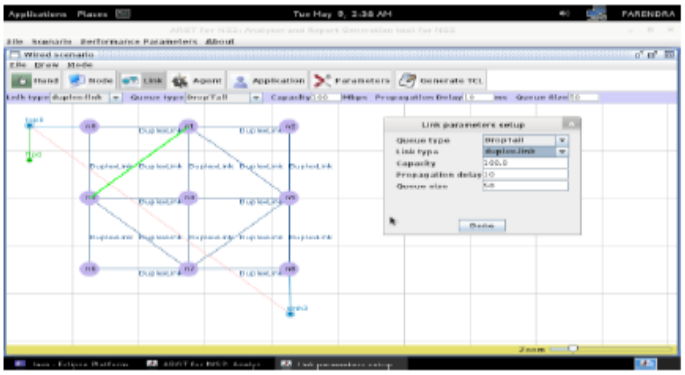


Figure 3 Wired scenario with definition of the connection parameters

First define an agent and then define the application that will use it. Then we can set other parameters like packet size, packet rate, etc. We can also define simulation parameters such as simulation time, trace file and name of the NAM file.

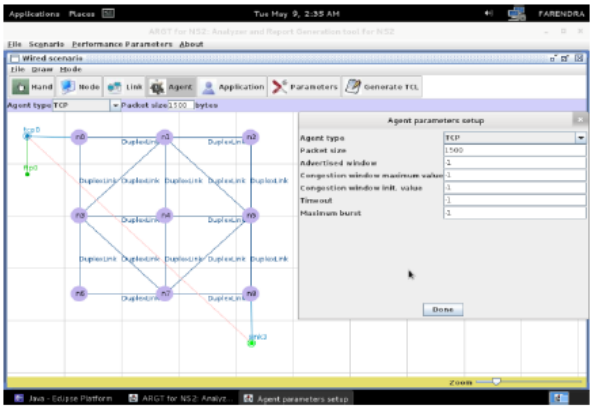


Figure 4 Wired scenario with definition of the configuration of the agent parameters

After created the complete scenario, you can now generate the report for the TCL script using the "Generate TCL" button. In the standard GUI toolbar there is a button for generating TCL. Provide the TCL script skeleton required for Network Simulator 2.

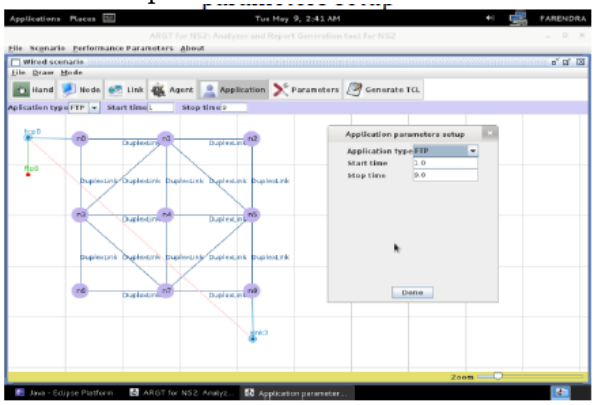


Figure 5 Wired scenario with definition of application parameter settings

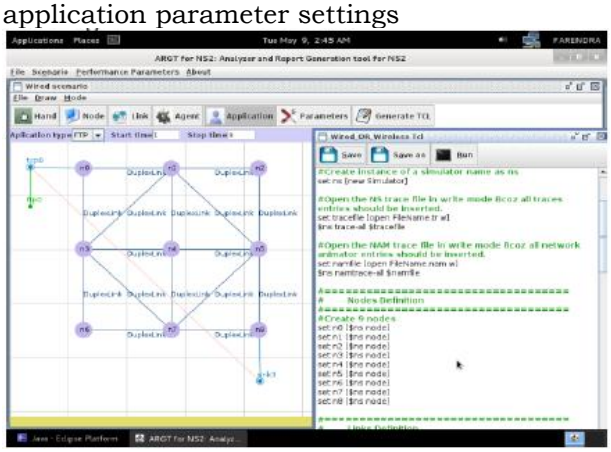


Figure 6 Generate TCL script report for wireframe scenario

We need to add our own logic without which the TCL code will be incomplete. Now that we've put our logic in the TCL skeleton code, we can now run it using NS2.

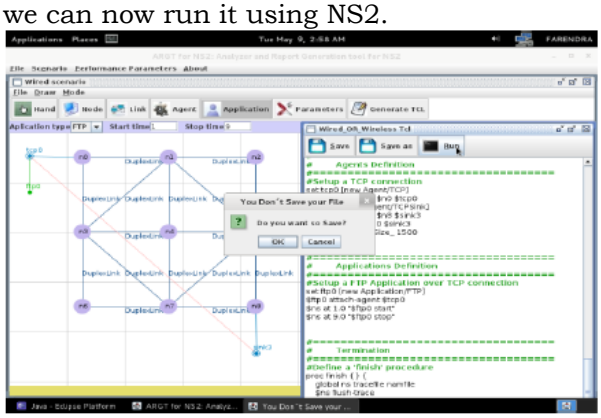


Figure 7 Generate a TCL script report and run it with NS2

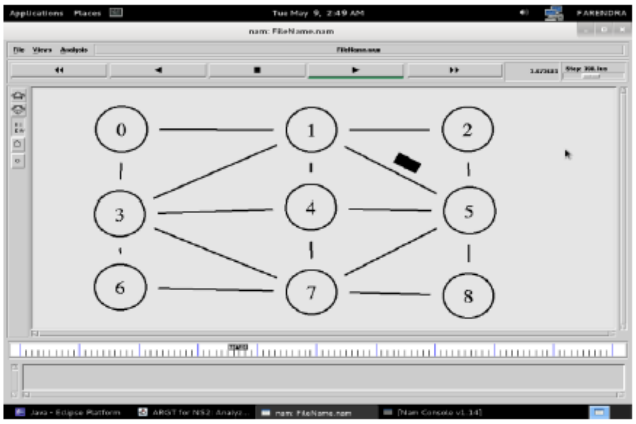


Figure 8 NAM for code generated from a simulated TCL script report in NS2

4.3 Statistical Analysis

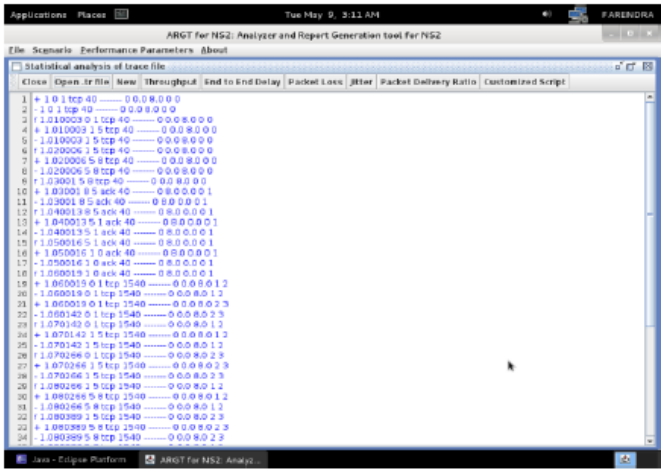


Figure 9 List of performance parameters

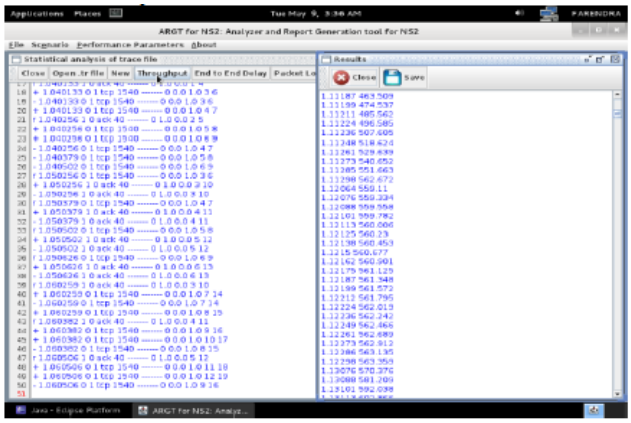


Figure 10 Statistical Analysis with XGraph Performance Metrics "Performance"

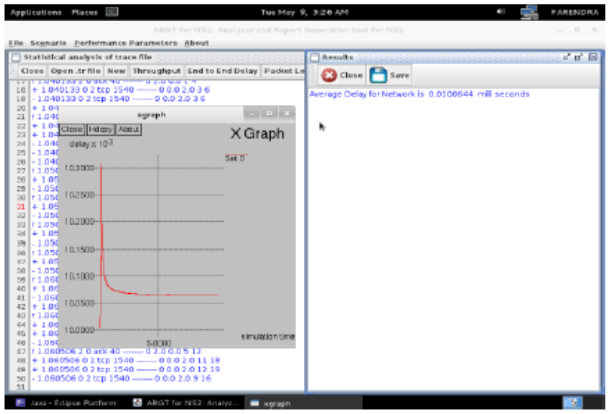


Figure 11 Statistical Analysis with XGraph Performance Metrics "Lag"

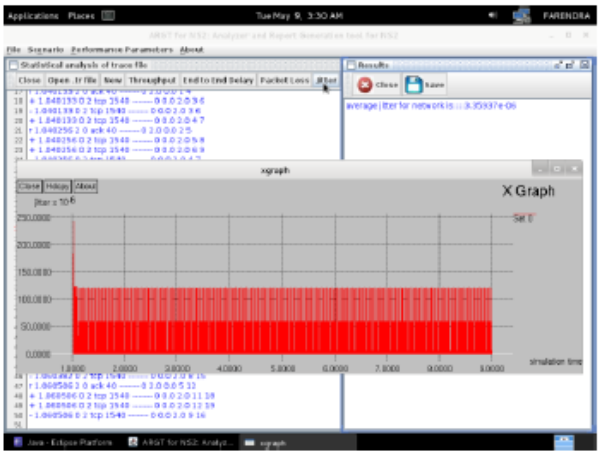


Figure 12 Statistical Analysis Using XGraph "Jitter" Performance Metrics

The above figure shows the animation of the tcl that was generated by clicking the Run tab. This raw data is used to perform a statistical analysis of the network topology. The GUI provides a file open function that requires us to select the trace file that we want to analyze. There are several tabs in the toolbar for statistical analysis of the trace file. Here get the results of the performance settings by clicking the Performance Settings tab. The results can be in the form of a graph (performance) or simple numerical results (packet loss). Below is the general flow of steps to perform a statistical analysis.

5. CONCLUSION

In this system, mainly the TCL script file generator, its growth towards the network design scenario, I will introduce the exact functions of the "network simulation analysis with the TCL script file generator" and work with its functions compared to NS-2 Generator2 (NSG-2) are very standardized) scenarios.

Therefore I present the structure of my project as "Network Analysis with NS-2 and NSG-2.1", which is somewhat identical to the previous NSG-2.1. However, other additional functions are provided with a graphical user interface (GUI). . The simulation system helps the user who is working on the project without programming. provides an easy-to-use way out of rendering simulations, analyzing simulation results, and avoiding common pitfalls.

REFERENCES

1. NeetuSikarwar"Performance Comparison Of Ad Hoc Network With Ns2 Simulator"-2015.
2. Payal, J. S. K. "TCP traffic based performance investigations of DSDV, DSR and AODV routing protocols for manet using ns2." Int. J. Innov. Technol. Explor. Eng 3.2 (2013): 2278-3075.
3. Gouse, Sheikh, and RhitulKumbhar. "Network Simulation with TCL Script Generator for NS-2."International Journal of Emerging Trends in Science and Technology 1.06 (2014).
4. Mohammad Reza Nouri rad, Reza Kourdy “Tools for Creating TCL script in Network Simulator 2 (NS-2)” – 2012.
5. Mukeshkumar, Ganesh Kumar “To Analyze and Compare Ring and MeshTopologies with Varying Traffic Patterns” IJSHER,2347-4890, 289,Volume 1, Issue 2, Jan 2016.
6. Naval KishorLodhi“Development and Validation of a NS-2 Protocol at Network Layer” IJARCSSE, ISSN: 2277 128X, Volume 5, Issue 6, June 2015.
7. Nikita, Shikha Gupta “Analyzing the Congestion and Flow Controlin UDP Protocol Using NS2”IJCSMC,ISSN 2320-088X,Vol. 5, Issue. 5, May 2016.

MATRIX AUTHENTICATION AND DASH MATRIX ALGORITHM FOR SECURED ELECTRONIC PAYMENT AND ATM TRANSACTIONS

V. Saroja[1]., B. Haritha[2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ donsaroja007@gmail.com)

2 Associate Professor, Department of H&S., Santhi Ram Engineering College., Nandhyala, AP., India.

Abstract: ***NFC (Near Field Communication) is a short-term remote matching innovation with an innovation gap of approximately 4 inches that operates in the 13.56 MHz repeat band at a speed of 106 kbps at 424 kbps. The combination of NFC with smart devices has expanded the reach of NFC, integrating information trading, profit disclosure, attribution, electronic payment and ticketing. We use the NFC innovation for registering ATMs. We provide a strong verification username, secret key, and NFC tag verification and shading password verification, and grid password verification. We also offer account balance display, transfer money, edit details: the user can take advantage of the additional benefits of ATMs, including customizing inquiries and changing points of interest.***

Keywords: ATM transaction, Dash Matrix algorithm, NFC tag, credit, money transfer, electronic payment, NFC transmitter, NFC receiver, non-NFC compatible phones

1 INTRODUCTION

A sensible and increasingly regular misfortune, including the break in computerized trading, is the taking or stealing of ATM cards. Unlike most flight methods, this implies the lack of an intrinsic defense of the framework and the ATM system itself. With a specific endpoint to overcome this natural shortcoming, we present a framework that uses a generally new innovation called NFC to provide security during the Share and use to implement. The ability of this company is to create the countermeasure against the theft of ATM cards and control the use of the ATM card by unauthorized persons. The additional component of this company is that no exchanges should be possible without separate cardholder information as an NFC exchange is taking place. To ensure the well-being and fairness of online payments for households, various banks have implemented a three-step validation process to verify online exchanges.

2 PROPOSED METHODOLOGY

This segment shows the proposed framework, configuration, and in-depth clarification of the basic procedures included. A review of the framework is shown in Figure 1.

2.1 Secure ATM exchanges with NFC

This method is used for faster and more reliable transactions without affecting the usage for ATM customers. This procedure is further divided into three subdivided procedures.

1. Client access via NFC tags: Each client has its own NFC tags. These labels contain your remarkable identification of each customer in the circuit. The customer should place the NFC tags near the NFC device so that the device can track the NFC tags. The beacons work correctly by avoiding at all costs from getting closer to the device by about 5 to 8 cm.

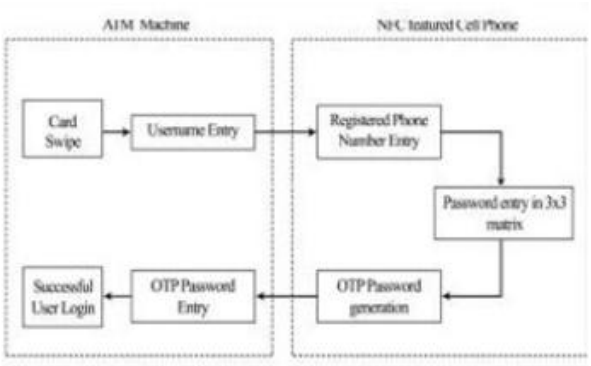


Fig. 1 Frame overview

2.2 Secure ATM exchanges with NFC

This method is used for faster and more reliable transactions without affecting the usage for ATM customers. This procedure is further divided into three subdivided procedures.

1. Client access via NFC tags: Each client has its own NFC tags. These labels contain your remarkable identification of each customer in the circuit. The customer should place the NFC tags near the NFC device so that the device can track the NFC tags. The beacons work correctly by avoiding at all costs from getting closer to the device by about 5 to 8 cm.
2. As soon as the frame differentiates the NFC tags, the customer can see the bank's POIs. However, the exchange and various rights are simply granted after the second security phase. NFC tags are approved on the server side.
3. Match-based authentication conspiracy: During registration, the client presents its

secret key. The minimum password length is 8 and can be referred to as a mystery pass. The Mystery Pass must contain a significant number of characters. Session passwords are created for this mysterious password. In the middle of the login phase, when the client enters its username, an interface consisting of a grid is displayed. The grid measures 6 x 6 and consists of letters in sequence and numbers. These are randomly placed in the network and the interface inevitably changes.

2.3 Examine NFC tags

The customer checks the NFC TAG by swiping the mobile phone over the ATM's NFC tag.

2.4 Matrix authentication

When the user authenticates the NFC tag, the user logs into the system. The next tab is the matrix authentication level. Below the matrix

Fig. 2 Matrix window

2.5 Algorithm

After the customer examines the NFC tag with an NFC mobile phone, the verification screen is displayed on the screen. The user must enter the example that demonstrates the secret word. The idea of the pattern password involves another calculation called the Dash Matrix Algorithm (DMA). The algorithm used in the matrix authentication system is shown below.

```
int[] pindex = new int[password.length]; int k = 0;
for (char pchar : password) { for (int i = 0; i < 6; i++) {
for (int j = 0; j < 6; j++) {
if (textMatrix[i][j] == pchar) { pindex[k] = (k % 2 == 0) ? i : j;
}
}
}
if (k % 2 != 0) {
sessionPassword +=textMatrix[pindex[k - 1]][pindex[k]];
}
k++;
}
out.print(sessionPassword + "<br/>" + pwd + "<br/>");
if (pwd.equalsIgnoreCase(sessionPassword)) { out.print("Login Successful using text<br>"); return true;
```

2.6 NFC tags

NFC tags are passive devices, ie they work without their own power source and are dependent on an incoming active device within range before being activated. The disadvantage here is that these devices cannot actually process it themselves. They are only used to transfer information to an active device such as a smartphone.

Fig. 3 NFC tag

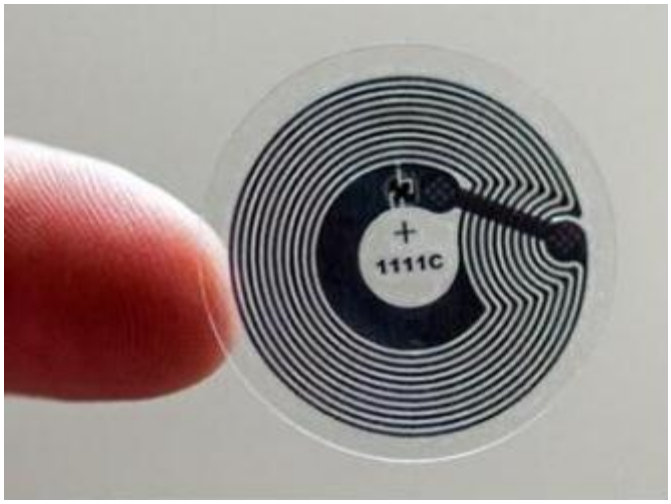


Fig. 4 Type 1 Tag

In order to supply these NFC tags with power, a current is generated in the passive device by means of electromagnetic induction. We're not going to be overly technical, but the basic

premise is that wire spools can be used to create electromagnetic waves, which can then be picked up by another wire spool and converted into electricity. This is very similar to the techniques used for wireless charging technologies, albeit much less powerful.

3 RESULTS

At Proposed System we use the NFC innovation for registering ATMs and provide username, password, NFC tag verification as well as secret password confirmation and password confirmation from the frame. In addition, we offer account balance, transfer money and edit details: the user can use the additional utility of the ATM, which includes query parameters and subtle item editing. We provide a strong username, a password for validation and confirmation of the NFC tag and confirmation of the shading password and confirmation of the password. Within the existing framework, the combination of NFC with shiny devices has led to an expansion of the scope of NFC. In particular, it is necessary to replace Visa in electronic subscription. In this way, safety concerns must be addressed in order to revive the NFC electronics system. To use NFC in electronic payments, security is essential.

4 CONCLUSIONS

In the proposed system, each customer has their extraordinary NFC tags. These labels contain your unique identification of each customer in the circuit. The customer should place the NFC tags next to the NFC device so that the device can track the NFC tags. Beacons work properly if they are avoided at all costs of about 5-8 cm near the device. As soon as the framework has identified the NFC tags, the customer can see the bank's special destinations, but can exchange and grant various rights immediately after the second security phase. NFC tags are approved on the server side. We use the NFC innovation for registering ATMs. Gradually, NFC security indicators characterize the organization of information trading, types of labels and security conventions, with an emphasis on NFC collection. NFC is a short-term innovation for distance correspondence. Because of its separation limitations, the innovation of short-term correspondence is significantly more secure than that of cable correspondence, which it certainly is not. If the match is made using the RF field using NFC, the information can be captured even if the clients stay close to the transmitter. In this area you will find the security requirements that NFC technologies meet for analyzing security risks.

REFERENCES

1. C.Balakumar, A.M.Adrean mel Clinton, J.Karthikumar “NFC ACCEPTANCE BY AN ADVANCED ATM MACHINE ” Proceedings of 4th IRF International Conference, Chennai, 9th March-2014, ISBN: 978-93-82702-64-1
2. Anusha Mandalapu, Daffney Deepa V, Laxman Deepak,Raj Anish Dev J "A NFC included three level confirmation framework for viable exchange and edited
3. version of ATM card blocking complexities" , 978-1-4799-6908-1/15/$31.00 ©2015 IEEE
4. Thivya.G, Amutha.C “Deployment of NFC for Security Purposes and Efficient Transaction in Real World” (An ISO 3297: 2007 Certified Organization) Vol. 3, Special Issue 2, April 2014
5. J. A. Ang, R. F. Barrett, R. E. Benner, D. Burke, C. Chan, J. Cook, D. Donofrio, S. D. Hammond, K. S. Hemmert, S. M. Kelly, H. Le, V. J. Leung, D. R. Resnick, A. F. Rodrigues, J. Shalf, D. Stark, D. Unat, and N. J. Wright. Unique machine models and intermediary structures for exascale figuring. In Proceedings of the first International Workshop on Hardware-Software Co-Design for High Performance Computing, Co-HPC '14, pages 25–32, Piscataway, NJ, USA, 2014. IEEE Press.
6. Bradford L Chamberlain, Sung-Eun Choi, Steven J Deitz, David Iten, and Vassily Litvinov. Composing client characterized area maps in Chapel. In CUG 2011, 2011.

N-GATEWAY FOR PRECISION AGRICULTURE MONITORING ON IOT CLOUD THROUGH WSN NETWORK

Y V Reddy., Satish Kumar, A

Assistant Professor, Department of H & S., Malla Reddy Institute of Technology., Maisammaguda., Medchal., TS, India (✉ yvreddy_mrit@gmail.com)

.

Abstract - The economies of developing countries like India which are mainly dependent on the agricultural sector. On the other hand, the growing population of the agricultural sector is faced with the problem of feeding everyone in the country. Other environmental factors are also responsible for the efficient growth in the quantity and quality of food from agricultural land. There is a loss of production due to the lack of accurate information and communications. In this proposed system using Internet of Things (IoT) and Wireless Sensor Network (WSN) technology, some of the problems can be minimized and the quantity and quality of food can be increased. In this article, the proposed system uses hardware such as n-Mote, n-Gateway and various sensors that detect atmospheric parameters related to agriculture and alarm trainers or the greenhouse keeper related to the environment, therefore the quantity and quality of the food can be increased. The cloud plays an important role in this proposed system.

Keywords: Internet of Things (IoT), Wireless Sensor Network (WSN), n-Mote, n-Gateway, Cloud.

1 INTRODUCTION

Food is the basic need of all people in this world. As the population grows, so does the need for food. And the agricultural sector needs to produce a large amount of the efficient quantity and quality of local food. In order to preserve the huge food products, the agricultural sector needs to be improved with new techniques and new technologies implemented locally. According to world statistics, India is in the Position 27 in food production as India still struggles to feed everyone in the country. Increasing the quantity and quality in agriculture with the help of IoT and WSN is known as intelligent agriculture or precision technology. The use of modern information and communication technologies (ICT) in agriculture leads to the third green revolution in the agricultural sector.

2. RELATED WORKS

Kwang-il Hwang et al. presented a document on the design and implementation of a gateway for wireless sensor elements for economic advice and management over the global location [1]. This article assigned the Sensor Element Gateway architecture for web management and details of how to implement it.Sirisha et al. presented a document on the wireless sensor element ZigBee-based remote agricultural monitoring system [2]. The system consisted of the network of wireless detection elements for ground surveillance and the remote information center. The sensor element node was developed using the JN5121 module and the IEEE 802.15.4 / ZigBee wireless microcontroller.Sonali et al. presented an article on monitoring the wireless sensor network with a smartphone application mainly based on Android [3]. The planned work of this project is to use centralized computer technologies and Android programming to develop the application.Prof. CH Chavan et al. proposed a wireless monitoring system for soil moisture, temperature and humidity using the zigzag in agriculture [4]. The proposed hardware system comprises an 8-bit AVR, a Bluetooth module, temperature, humidity and soil humidity sensors and an LCD display. The system is inexpensive and energy efficient so everyone can afford it. Prabha et al. presented an article on real-time atomization of the agricultural environment for social modernization of the Indian agricultural system using Arm 7 [5]. This device leverages the integration of cabling and Wi-Fi techniques

and the ARM controller to ensure normal monitoring under the environmental conditions of the farm, and also provides the critical precautions that are taken for the performance and growth of the farm have to contemporary agriculture.

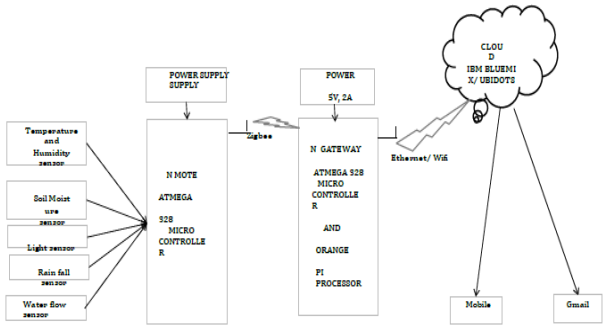


Fig. 1: Functional diagram of smart agriculture

3. OBJECTIVES

The main objectives of the proposed system are listed below:

- Increase of productivity.
- More safety.
- Simpler farming practices.
- Immediate intervention 24 hours a day.
- Advanced lifestyle.

4. PROPOSED SYSTEM

The main reason for precision farming is to increase the quality and quantity of crops. For this purpose, IoT and WSN are used to create the smart grid for an efficient network. The sensors for measuring various parameters of the agricultural system that are used at the sites. These sensors are internally connected to the microcontroller (N Mote) that controls the sensors. A gateway is used to connect two different networks that are connected to the Internet via Wi-Fi or Ethernet. The data from the sensors is sent to the gateway and then to the cloud. When certain thresholds are reached, the data is sent to the respective destination.

The proposed system works in three departments. That is, the n-mote section, the n-gateway section and part of the cloud.

4.1 Implementation

The sensor data is collected by sensors that measure the physical parameters of the atmosphere at various voltage levels, which in turn are converted into suitable formats for sending the data to the processor. The sensor data are sent to the N-Mote (AtMega 328 microcontroller). Five sensors are used here, namely digital humidity and temperature (DHT11), soil moisture, water flow, rain and light sensor (LDR). The sensors measure the physical parameters in relation to the environment and send the data to the n-Mote. The received data is processed and transmitted to Xbee (IEEE 802.15.4 protocol) in order to send the data from N-Mote to N-Gateway, as AtMega 328. The microcontroller does not support Wi-Fi or Ethernet functions. The data is sent to the Xbee receiver at the N gateway end.

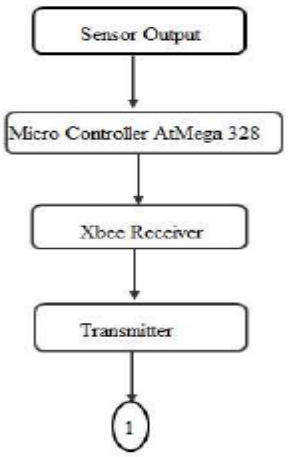


Fig. -2: n-Mote section

Sensor data received from the N-Mote Xbee transmitter is processed and displayed on the laptop or desktop computer connected to the N-Gateway. Elsewhere, the received data is forwarded to the Pi processor to send the data to the cloud using a Python script over Ethernet or Wi-Fi.

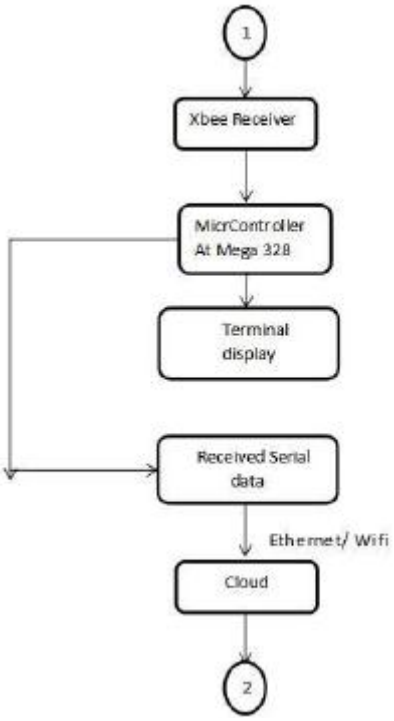


Fig. 3: Section n-Gateway

The sensor data received in the cloud is saved and a database is created. Once the sensor data reaches the threshold, the rest is sent to the mobile phone or via email.

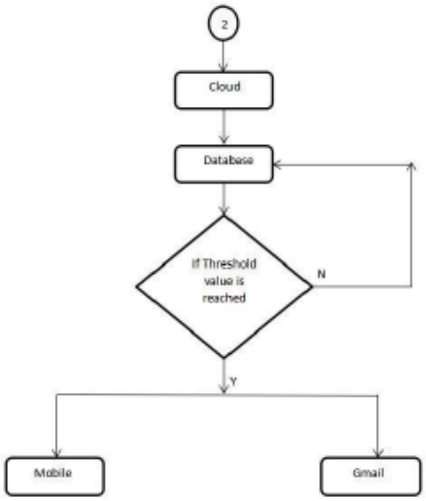


Fig -4: Cloud section

5. RESULTS

In this section we discuss the results of the Mote sensor, the physical parameters measured by the sensors and sent to the cloud to make the greenhouse application decisions.

Fig. 5: Temperature measurement in the cloud

Fig. 6: Measurement of the humidity in the cloud

Fig. 7: Light measurement in the cloud

Fig. 8: Rain measurement in the cloud

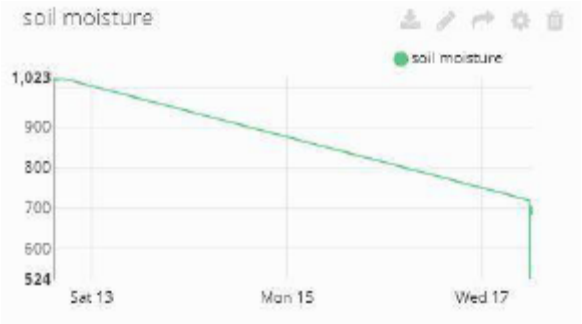


Fig. 9: Temperature measurement in the cloud

6. CONCLUSION

This study developed a conceptual model and system to be designed using sensors, engines, and gateway and communication protocols to form a real-time application. The cloud plays an important role in decision making, data collection and data maintenance in order to make important decisions in the system. Further research is required to keep the entire system running automatically under all conditions and without human intervention.

REFERENCES

1. M.K.Gayatri, Dr.G.S.Anandha Mala, J Jayasakthi, “Providing Smart Agricultural Solutions to Farmers for better yielding using loT”, In Technological Innovation in ICT for Agriculture and Rural Development TIAR 2015.
2. Zhou, Zhongwei, and Zhongyi Zhou. "Application of internet of things in agriculture products supply chain management." In Control Engineering and Communication Technology (lCCECT), 2012 , pp.259-261, IEEE, 2012.
3. Sinung Suakanto, Ventje J. L. Engel, Maclaurin Hutagalung and Dina Angela, “Sensor networks data acquisition and task management for decision support of smart farming” International Conference on Information Technology Systems and Innovation (ICITSI), 2016 .
4. Rui, Jiang, and Sun Danpeng. "Architecture Design of the Internet of Things based on Cloud Computing." Seventh International Conference on Measuring Technology and Mechatronics Automation (lCMTMA),

BIOMETRIC IDENTIFICATION OF PERSON MATCHING THROUGH FINGER KNUCKLE USING GABOR FILTER AND KNN CLASSIFIER

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: ***Fingerprints can be incredibly beneficial to a person's identity. FKP is a new biometric modality that will offer researchers a broad field of action over the next few years. In this system we present a joint identification method using subspace techniques. In the proposed system we use the three subspace techniques. We first use the Gabor filter in preprocessing to remove noise from the captured image and we get the noise free image. Second, we use PCA for feature extraction and finally the LDA and Knn classifier for matching purposes. The result obtained from the knn classifier and the LDA algorithm gives a recognition rate of approximately 98%. It also offers high efficiency compared to other methods.***

Keywords: phalanx, LDA, PCA, Gabor filter, image processing, feature extraction, identification

1 INTRODUCTION

In ancient times, conventional modes such as password device, PIN code range system and ID card device are used for the authentication cause. The biometric device is mainly used in male or female authentication devices than in conventional methods. Genetic developments such as fingerprint, face, iris, palm print, hand geometry, finger vein and hand vein are used as biometric systems. Biometric behaviors such as palm print, fingerprint, hand vein, and hand geometry are widely used due to the person's over-acceptance. The photo shows the folds and folds of the membrane, the outer area of the finger joints is very pronounced. Therefore, this biometric feature is used as a characteristic biometric device [4]. The inner surface of the knuckle impression is often used for object preservation. Hence, it is not always easily damaged by an intruder. Criminal sports are not linked to the fingerprint of the ankle and are therefore widely recognized by consumers [13]. Joint surface tensions do not occur on the sensor tool and therefore cannot be cast without difficulty. It has a very wealthy texture and is used as a great biometric device. In these paintings, a feature fusion approach to the biometric fingerprint scheme that is close to everyone is offered.

2. PROPOSED METHODOLOGY

The proposed authentication system processes the database with an "n" number of images, i. H. A system is designed for one-to-many identification. A system only uses a webcam or smartphone as part of the hardware [2]. The system is divided into two main modules: registration and identification.

The system can be fully understood using the system block diagram shown in Figure 2. The proposed work focuses on the advancement of a mechanized strategy for removing fingerprints and reflections from the joints of the posterior surface of the fingers and using them for an individually identifiable sanity test.

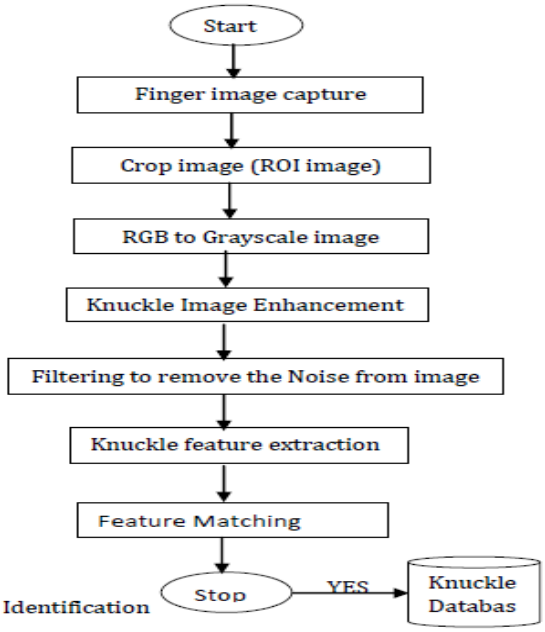


Fig. -1: Flow chart for the suggested identification of the articular surface

2.1 Block diagram

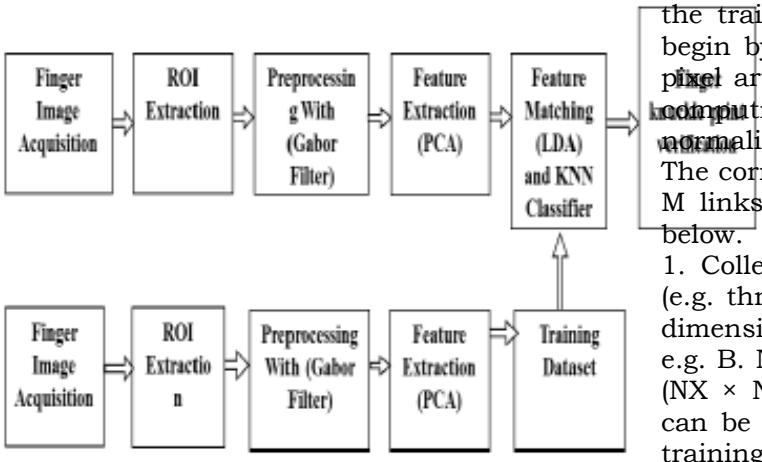


Fig. -2: Functional diagram of the proposed system

2.2 Suggested Techniques

- Gabor filter
- PCA
- LDA

2.1.1. Gabor filter:

Gabor filter Implements one or more turns of an input image with a two-dimensional Gabor function:

Real

$$g(x, y; \lambda, \theta, \varphi, \sigma, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) cos\left(2\pi \frac{x'}{\lambda} +\right.$$

Where,

To display a Gabor function, select the "Gabor function" option under "Output image". The Gabor function for the specified values of the parameters "wavelength", "orientation", "segment offset", "aspect ratio" and "bandwidth" can be calculated and displayed as an image of the intensity map in the output window. (Soft and dark gray colors correspond to advantageous and terrible characteristic values, respectively.) The image in the output widow is the same size as the captured photo: for example, type image octagon.jpg to get an image output of a hundred length with 100. If the value lists "Orientation (s)" and "Segment offset (s)" are correct, the simplest primary values from these lists can be used.

2.1.2. PCA

Principal component analysis (PCA) determines the basis vectors that cover an optimal subspace in order to minimize the root mean square error between the projection of the training images in this subspace and the original images. We call this set of optimal basis vectors eigenarticulations because they are simply the eigenvectors of the covariance matrix calculated from the vector images in the training set. The feature extraction steps begin by first representing each of the N × M pixel articulation images by a vector and then computing its covariance matrix of these normalized vectors Θj

The correct link search algorithm for images of M links with similar dimensions is explained below.

1. Collect a number of sample joint pictures (e.g. three joint pictures for each person). The dimensions of all images should be the same, e.g. B. NX x NY. An image can be stored in an (NX × NY) × 1 dimensional [T] matrix, which can be viewed as an image vector. Hence the training set of image vectors of size (NX × NY) × M,

$$\{\Gamma i \mid i = 1, 2 \ldots\ldots M\} \quad (2)$$

Where M is the average number of images. To find the average image of a group of images,

$$\psi = \frac{1}{M}\sum_{i=1}^{M} \Gamma_i \quad (3)$$

2. To search for biased images [Img1-Avg, Img2-Avg, Imgn - Avg],

3. Calculate the covariance matrix

$$C = AAT \quad (5)$$

$$C = \begin{bmatrix} c(1,1) & \ldots & c(1,d) \\ \vdots & \ddots & \vdots \\ c(d,1) & \ldots & c(d,d) \end{bmatrix} \quad (6)$$

Where, A= [øi, ...,øm]

The problem with this approach, however, is that we cannot complete this operation on a group of images because the covariance matrix is extremely large.

For example, the covariance matrix for a common image of size NX × NY pixels is size (P × P), where P is (NX × XNY). This covariance matrix is very difficult to use because of its enormous size, which adds complexity to the computation. It is very difficult or practically impossible to store this matrix. Finding this matrix also requires significant computational requirements. To solve this problem, we first compute the matrix L.

$$L = ATA \quad (7)$$

And then find the eigenvectors [V] associated with it

$$VX(X = 1\ldots\ldots, M) \quad (8)$$

The eigenvectors of the covariance matrix C can be found by

$$U = [u1\ldots\ldots, um] \quad (9)$$
$$= [Ø1\ldots Øm][v1,\ldots\ldots,vm] \quad (10)$$
$$= A \cdot V \quad (11)$$

Where UX (X = 1 …… .., M) are eigenvectors for C. With these eigenvectors we can form eigen connections. The joint itself has a numerical value that is classified and identified by the LDA.

4.1.3. LDA:

Linear discriminant analysis has been used successfully as a classification technique for a number of problems, such as: B. speech recognition; Face recognition. While PCA regards the training data set as an entity, the main goal of LDA is to find an efficient way to represent the vector space using the class information (the class is defined as a collection of data belonging to a particular entity, e.g. a collection of images of a person) [7-9]. The FK images of the training set are divided into corresponding classes. LDA then computes a set of vectors W as follows:

$$W = \max\left|\frac{W^T S_b W}{W^T S_w W}\right| = \max\left|\frac{S_b}{S_w}\right|$$

3. CLASSIFICATION AND IDENTIFICATION USING KNN CLASSIFICATION

3.1. Classifier K- nn

During the classification, a pattern is recognized and compared with the predefined pattern in the database, and the corresponding features are identified. The training should be done with the predefined characteristics and the characteristics of the training and the test are compared. The test function is our input image. If the features match, they will be recognized. The k-nn classifier is used here. The K nearest neighbor classifier is a robust method that is used for matching. The k-nearest neighbor pattern classifier (k-nn) is an efficient learner to general pattern recognition domains.

4. RESULT

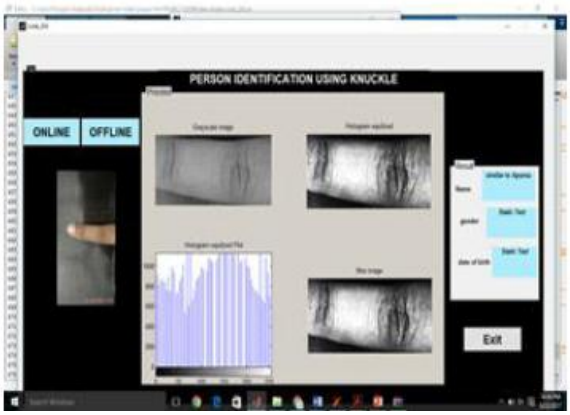


Fig. -3: Final user interface

The proposed idea guarantees improved security and efficiency compared to the traditionally used biometric identification.

5. CONCLUSION

This article presented a new approach to the subspace technique for personal authentication using the posterior surface of the finger joint. This system compares the user's joint with the joint database of the joint captured with a webcam, the outline part of two images. You stated that if the two match perfectly, the match percentage is 96.7%.

REFERENCES

Kyi Pyar Zaw, Aung Soe Khaing, "Implementation of Contactless Finger Knuckle Identification System," IJSETR, vol. 3, Issue 6,June 2014. (references)

Shubhanda Sonawane, Verifying Human Identities Using Major and Minor Finger Knuckle Pattern, vol.5, Issue2, Feb 2016.

D. L. Woodard, P. J. Flynn, "Finger surface as a biometric identifier", Computer Vision and Image Understanding, pp. 357-384, vol. 100, Aug. 2005.

Kumar, A., Ravikanth, C., "Personal authentication using finger knuckle surface," IEEE Trans. Information Forensics and Security 4(1), 98–109. 2009.

M. Chora´ s and R. Kozik, "Contactless palmprint and knuckle biometrics for mobile devices," Pattern Anal. Applicat., vol. 1, no. 15, pp. 73–85, 2012.

ATTRIBUTE-BASED ENCRYPTION FOR PRIVACY PROTECTION OF BIG DATA USING HOMOMORPHIC ENCRYPTION AND RING SIGNATURE

T. Sudha[1]., M. Dhange[2].,

1 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India (✉ sudhathulluri@gmail.com)

2 Associate Professor, Department of H&S., Halakatta College of Engineering and Technology, Vijayapur., Karnataka., India.

Abstract -In the past few years, big data has become a hot research topic. The increasing amount of huge information also increases the possibility of invading people's privacy. Since the large amount of information requires a high processing power and a large storage space, distributed systems are used. Because multiple parties are involved in these systems, the risk of data breaches increases. There are a variety of privacy protection mechanisms that have been developed to protect privacy in completely different phases (e.g. information generation, information storage and information processing) from a big data lifecycle. The aim of this project is to create a complete synthesis of the mechanisms for safeguarding privacy in big data and to illustrate the challenges of the existing mechanisms. Importantly, during this project we are proposing a new mechanism for protecting big data privacy called ring signing.

Keywords: big data, attribute-based encryption, identity-based encryption, homomorphic encryption and ring signature

1 INTRODUCTION

The enormous amount of information that is generated from various sources in various formats at incredibly high speeds is known as big data. Big data has become a really active place for analysis in the past few years. The speed of information generation is increasing rapidly, making it difficult to manage with traditional strategies or systems. Meanwhile, large amounts of knowledge can be structured, semi-structured, or unstructured, which creates additional challenges once data storage and processing tasks are performed. To that end, we would like new ways to store and analyze data in real time.

The user's privacy can be violated under the following circumstances:

• Personal information from users in combination with external records can lead to new facts about users. These facts can be secret and may not be passed on to third parties.

• Sometimes personal information is collected that adds value to the company. For example, a person's shopping habits can reveal a great deal of personal information about the user who will be shopping online.

• Sometimes sensitive information is stored and processed in a location that is not properly protected. In such cases, information leaks can occur during the storage and processing phase.

Protecting privacy in big data can be a rapidly growing area for analytics. This document introduced the basic idea of protecting privacy in big data.

2. LITERATURE SURVEY

As mentioned earlier, the tools and techniques used to process this data also need to be updated as the size and diversity of the data grows rapidly. Here are some existing privacy techniques.

V. Goyal, O. Pandey, A. Sahai, and B. Waters worked on an article suggesting an attribute-based encryption scheme. This is one of the encryption techniques that consistently guarantee the confidentiality of big data in the cloud storage system.

With attribute-based encryption, access policies are defined by the owner of the data and information is encrypted according to these policies. Information can only be decrypted by users whose attributes meet the access policies set by the owner of the data. When it comes to big data, data access policies often need to be changed because the owner of the data may need to share it with different organizations. The current attribute-based encryption does not support updating policies. Updating the policy is a difficult task with this type of encryption scheme. The reason for this is that the data owner no longer keeps the local copy on his system once the data has been moved to the cloud storage. If the data owner wants to update the policy, they must transfer the data to the local system, re-encrypt the data with the new policy, and save it again on the cloud server. This leads to a very high communication overload and a high computing effort [6].

X. Boyen and B. Waters suggested identity-based encryption in their article. Identity-based encryption is an alternative to public key encryption proposed to simplify the key management system in a certificate-based public key infrastructure, using human identities such as email address or IP address as the public key. The identity-based encryption scheme has been proposed to protect the privacy of the sender and recipient. Identity-based encryption does not support updating the ciphertext recipient.

C. Gentry carried out a study on homomorphic encryption.The public cloud is more prone to data breaches due to virtualization and multi-tenancy. Different cloud users can share the same physical storage space. In such a scenario, the likelihood of data loss is also high. One way to protect data in the cloud is to first encrypt the data and store it in the cloud for data protection reasons. Then let the cloud do calculations for the encrypted data. Fully homomorphic encryption is the type of encryption technique that allows you to compute functions for encrypted data. Given only the encryption of a message, encryption of a function of that message can be obtained by calculating directly on the encryption. The homomorphic encryption guarantees confidentiality. The disadvantage, however, is the complexity of the computation, which is sometimes very difficult to implement with existing technologies.

3. PROPOSED SYSTEM

In the proposed system, a new data protection system is introduced, namely the Ring company. The ring signature is the file authentication system for closed groups, in which the owner of the group data can securely release his files within the group without external conclusions. At the same time, the integrity of the file is preserved. The ring signature is created for each of the files. Using ring signature, group members can successfully decrypt the file and download it from Hadoop.

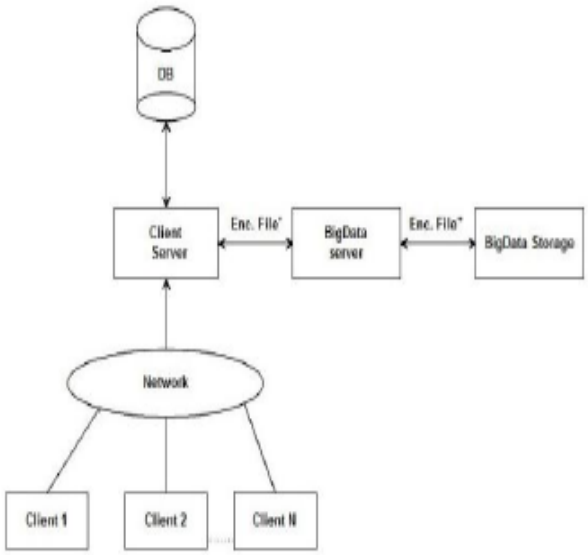


Fig. 1 : Proposed system architecture

The previous architecture explained how we use ring signatures to keep big data secure. The administrator creates a group by collecting your username. Then make security keys available to all users in the group. When client1 sends the file, it is saved on the client's server. A database is managed on the client server. This file is then encrypted with the ring signature and sent to the big data server. The file is encrypted a second time before it is moved to big data storage with the AES key. If someone wants to download the file, they have to download the ring signature. Otherwise you will not be able to download the file from big data storage.

3.1 Create ring signatures

The user receives the public keys of all members in the user group. Then the hash code for the download file is generated. To do this, use the hash code XOR with the public keys of all members in the user group. The end result of the XOR operation is SecureMD (Secure Message Digest). Then write the resulting SecureMD to the file used to create the protected file. Then encrypt the protected file with the download user's private key. The encrypted file is called Download File Ring Signature. After creating the ringtone signature, the user sends the ringtone signature file to the selected group members via email.

3.2 File encryption

Get the AES key

Encrypt the downloaded file AES encryption technology.

3.3 File Decryption Process

Get the AES key

Decrypt the downloaded file technique AES decryption

3.4 Checking the ring signature

The target user receives the public keys of all members in the user group. Generate the hash code for the downloaded file. Then perform the XOR operation of the hash code with the public keys of all members present in the user group.

4 RESULTS

The end result of the XOR operation is SecureMD (Secure Message Digest), let's call it SecureMD1. Decrypt the ring signature file with the public key of the downloaded user and get the SecureMD. Let's call it SecureMD2. Compare SecureMD1 and SecureMD2. If they match, the ring signature verification was successful and the file is successfully uploaded to the customer's system. Otherwise, the ring signature verification process will fail and an error message will appear stating that the ring signature does not match.

5 CONCLUSION

The amount of data is increasing day by day and it is impossible to imagine new generation applications without building and running algorithms based on the data. We examined the privacy challenges at each stage of the big data lifecycle and discussed some of the advantages and disadvantages of existing privacy technologies in the context of big data applications. Much work has been done to protect user privacy from the data generation to the data processing phase. However, there are still some unanswered questions and challenges.

Sometimes data pertaining to an organization doesn't have enough information to find useful information in that area, and collecting this data can be expensive or difficult due to legal restrictions and fears of confidentiality violations. To solve these problems, we need to develop distributed analytics systems that ensure data protection and are able to process different data sets from different organizations while maintaining data protection for each data set. Multi-part secure computing techniques such as homomorphic encryption can be implemented to address these problems. The greatest challenge when implementing homomorphic encryption in the context of big data analysis is to keep the computing effort as low as possible.

REFERENCES

1. Z. Xiao and Y. Xiao, ``Security and privacy in cloud computing,'' IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 843_859, May 2013.
2. S. Singla and J. Singh, ``Cloud data security using authentication and encryption technique,'' Global J. Comput. Sci. Technol., vol. 13, no. 3,pp. 2232_2235, Jul. 2013.
3. J. Manyika et al., Big data: The Next Frontier for Innovation, Competition, and Productivity. Zürich, Switzerland: McKinsey Global Inst., Jun. 2011, pp. 1_137.
4. Katal, M. Wazid, and R. H. Goudar, ``Big data: Issues, challenges, tools and good practices,'' in Proc. IEEE Int. Conf. Contemp. Comput., Aug. 2013, pp. 404_409.
5. V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute- based encryption for _ne-grained access control of encrypted data,'' in Proc. ACM Conf. Comput. Commun. Secur., Oct. 2006, pp. 89_98.
6. J. Bethencourt, A. Sahai, and B. Waters, ``Ciphertext-policy attributebased encryption,'' in Proc. IEEE Int. Conf. Secur. Privacy, May 2007, pp. 321_334.
7. K. Yang, X. Jia, and K. Ren, ``Secure and verifiable policy update outsourcing for big data access control in the cloud,'' IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461_3470, Dec. 2015.

ENCRYPTION OF MEDICAL IMAGES FOR SECURED USER DATA TRANSFER USING HYBRID DWT-SVD TECHNIQUE REVERSIBLE WATERMARKING

Vazralu, M
Associate Professor, Department of CSE., Malla Reddy College of Engineering & Technology., Maisammaguda., Medchal., TS, India (Email: vazralu.munnagi@gmail.com)

Abstract: ***This document is the combination of a reversible watermark and an encryption method for more security, robustness and confidentiality of medical images. When embedding watermarks, a two-step digital wavelet transform (DWT) is applied to the original cover image. The LH1 and LH2 sub-band coefficients obtained after applying DWT are selected for the watermark. The two sub-bands are divided into 4 × 4 matrices and Singular Value Decomposition (SVD) is applied. The watermark in the form of an image or text is converted into a binary format and encrypted. The encrypted watermark bits are embedded by changing the Singular Value Table (SV). Then reverse SVD and reverse DWT are applied to form the watermark image and then the image is encrypted for security reasons. In the watermark extraction process, the watermark is extracted from the SV matrix by reversing the embedding process. After extraction, the cover picture is reconstructed without using the original cover picture. The proposed system is simulated and the results analyzed using various performance measures. The experimental results show that the proposed system has better robustness and insensitivity to various attacks such as noise, harvesting and compression attacks.***

Keywords: watermark, DWT-SVD, medical image, reversible watermark, encryption, security

1 INTRODUCTION

The digital communication system has facilitated the transmission of digital data through the communication network. This simple handling guarantees no security problems. In order to carry out highly secure transmissions of this digital data, secret data is usually embedded in this original data. This process is especially popular with images known as watermarks. The watermark system is mainly used to ensure data ownership, confidentiality and reliability. Image reliability plays an important role in military and medical applications. In medical applications in particular, medical images are transmitted through notification and remote diagnosis. When patient data is transmitted, it is confidential, so that the patient identification, the hospital logo or other important information can be included in the image as text or as an image (binary image). . The watermark can be visible or invisible. The basic characteristics of the tattooing method are robustness, capacity, imperceptibility and security.

2. RELATED WORKS

This section summarizes the various works related to the watermark algorithm that applies singular value decomposition and discrete wave transformation. In [3] a robust watermarking method for images is proposed, which combines the technology of SVD, DCT and SVD. HL The middle frequency band is selected after DWT has been applied to the input image to accommodate the watermark. Kumar et al. in [4] proposed a watermarking method based on SVD and DWT. 3 DWT levels were used in this method. The watermark is then embedded in diagonal elements of the singular matrix of the original input image. Medium frequency bands (LH or HL) selected for the watermark embedding process. In [2] Amith et al. proposed a robust watermarking method by combining DWT, DCT and SVD. The first step is to decompose the original image into a DWT LL transform (low frequency band) of the first level. The next step is to mark the transformed image with SVD and DCT. The watermark values are then integrated into the singular matrix values of the original cover image. To get the watermark image, the inverted SVD is applied to the V, U and the modified vector S, then the inverted DWT and the inverted DCT are applied. Currently, the implementation of block image watermarking techniques is of interest because of their advantages, one of which is the ability to process each block individually and increase capacity.

3. PROPOSED LOCKING AND LABELING PROCEDURES

In this section we explain our proposed scheme of discrete wave transformation in combination with a block-based singular value decomposition for medical image watermarks. Patient data or hospital logo (watermark) and watermark image are encrypted for additional security.

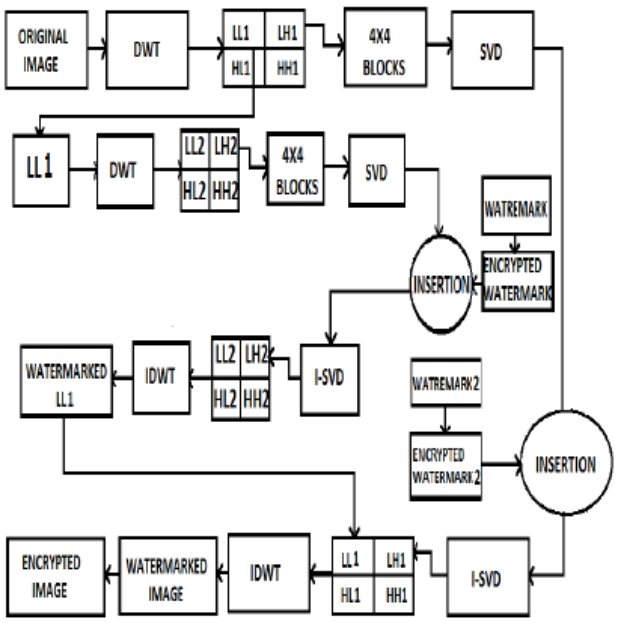


Figure -1: Block Diagram Of The Proposed Method

Embedding process for watermarks

Step 1: Take the input image (CT or any medical image).

Step 2: The two-stage discrete wave transformation ("Daubechies") is applied to the input image.

Step 3: For better imperceptibility and robustness, we selected the LH1 and LH2 subbands and divided them into non-overlapping 4x4 sub-blocks.

Step 4: Singular Value Decomposition (SVD) is applied in each 4x4 block to obtain a singular matrix.

Step 5: The watermark to be inserted (text or image) is converted to binary format and encrypted.

Step 6: The watermark bit (W) is inserted into the diagonal elements of the singular value table (SV) according to the insertion process.

Step 7: Inverse SVD is applied including the modified singular matrix.

Step 8: Reverse DWT applied to get the watermark image.

Step 9: The watermark image is encrypted for added security.

3.1 Insertion Process

```
S-Singular matrix of size 4x4 obtained after applying SVD
W-Watermark bit
If W==1
  q=(S(1,1)+(3,3))/2;
  if S(2,2)<=q;
    qq=q-S(2,2);
    S(2,2)=S(2,2)+qq+1;
  else
    S(2,2)=S(2,2);
  end
else if W==0
    if S(2,2)>q
      qp=S(2,2)-q;
      S(2,2)=S(2,2)-qp-1;
    else
      S(2,2)=S(2,2);
    end
```

3.2 Watermark extraction process

Step 1: The watermark image is decrypted and the two-stage discrete wave transformation ("Daubechies") is applied to the watermark image.

Step 2: The sub-bands LH1 and LH2 are selected and divided into non-overlapping 4x4 sub-blocks.

Step 3: Singular Value Decomposition (SVD) is applied to each 4x4 block to obtain a singular matrix.

Step 4: The watermark is extracted from the diagonal elements of the singular matrix according to the extraction process.

3.3 Extraction Process

```
S-Singular Matrix
W-Watermark bit
q=(S(1,1)+S(3,3))/2;
  if S(2,2)>q
    qq=S(2,2)-q;
    S(2,2)=S(2,2)-qq-1;
    W=1;
  else if S(2,2)<=q
    qp=q-S(2,2);
    S(2,2)=S(2,2)+qp+1;
    W=0;
  End
```

Step 5: The extracted watermark (W) in each block is concatenated and decrypted, the resulting watermark (binary form) is converted to the original form.

Step 6: Inverse SVD is applied after extraction using a singular matrix.

Step 7: An inverse discrete wave transform is applied to obtain the restored image.

4. EXPERIMENTAL RESULTS AND DISCUSSION

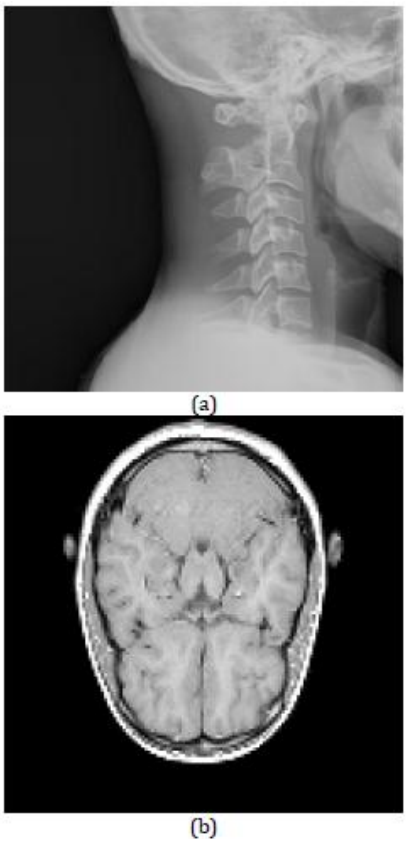


Figure -2: (a) and (b) CAPTURING MEDICAL IMAGES

The proposed scheme is simulated in MATLAB2013a using two medical images as test images shown in Figure 2 and a watermark (image and text) shown in Figure 3. The experiment is carried out by adding a watermark to the images. Medical entry.

The resulting watermark image, extracted watermark, and reconstructed images are shown in Figures 4 and 5 with their PSNR and BCR values. It is important to get good PSNR and BCR values regardless of the domain and method of the watermark. Indeed, this is essential in the medical imaging industry. The following are some of the performance metrics calculated for the proposed system.

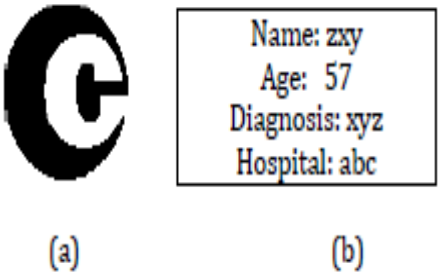


Figure -3:(a) Watermark (Image) (B) Watermark 2 (Text)

P (Si) is the histogram number of an image

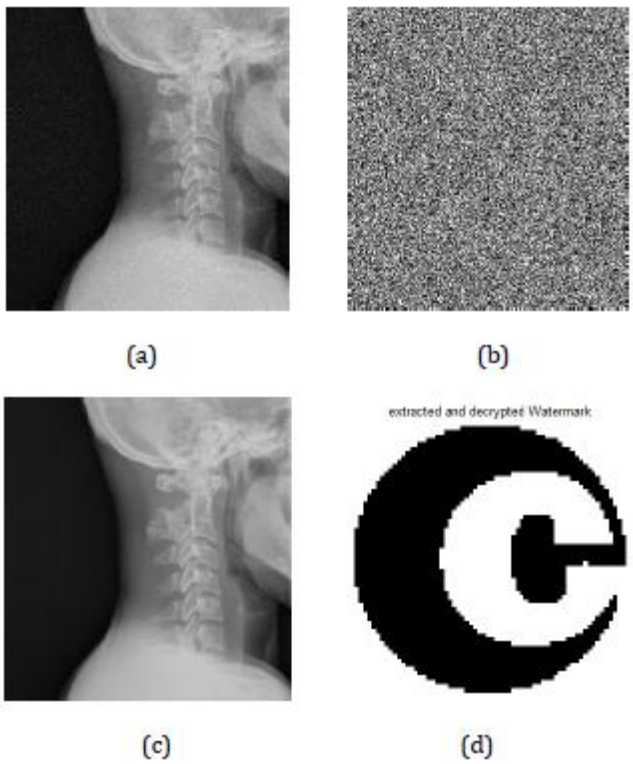


Figure -4:(a) Watermarked Image (PSNR=55.67dB) (b) Encrypted Image (Entropy=7.89 (c) Extracted Image (PSNR=61.03dB) (d) Extracted Watermark (BCR=0.9998)

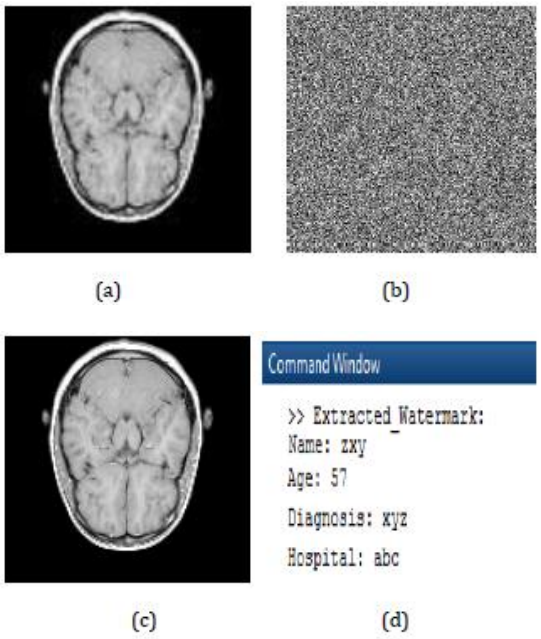


Fig -5: (a) Watermarked Image (PSNR=53.67dB) (b) Encrypted Image (Entropoy=7.68) (c) Extracted Image (PSNR=60.14dB) (d) Extracted Watermark (BCR=1)

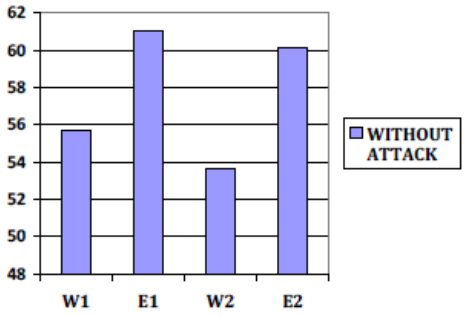


Chart -1: PSNR values of watermarked (w) and extracted (e) images without any attack
W1 & E1 - Figure 2 a , W2 & E2 - Figure 2 b

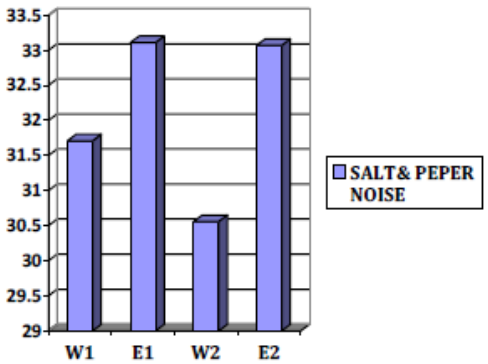


Chart -2: PSNR values of watermarked and extracted images against salt & pepper noise attack

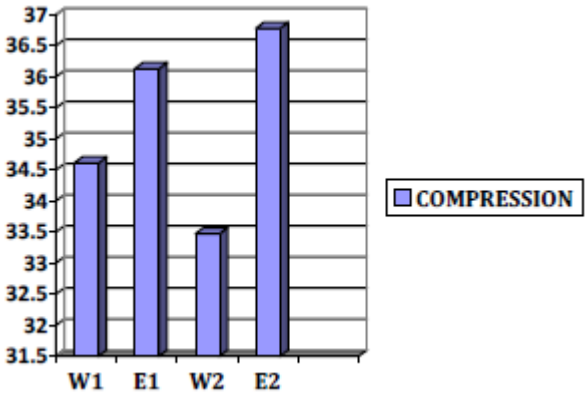


Chart -3: PSNR values of watermarked and extracted images against compression attack.

The most common attacks are selected to analyze the robustness of the proposed system. These are JPEG compression attacks, salt and pepper sounds, and clipping. After attacking the same medical images, we tried to extract our watermark and reconstruct the original image. The PSNR and BCR values of the simulated results are shown in FIGURE 1-4.

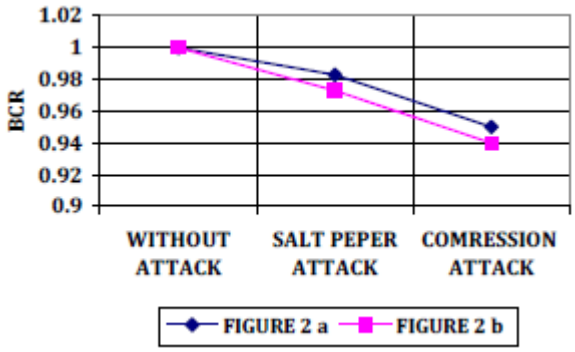


Chart -4: BCR values of the watermark against various attacks

The goal of this calculation is to determine the level of robustness of our algorithm to withstand various attacks. Based on the results, our proposed algorithm is more robust against various attacks with better BCR values and the cover images are reconstructed with good PSNR values.

5. CONCLUSIONS

This article introduces a block-based reversible encryption and watermarking scheme for DWT-SVD hybrids to ensure the confidentiality, robustness and security of medical images in transit. The result shows that the robustness of our proposed scheme against various attacks is high. Unlike most watermark designs, the cover photo is reconstructed with better quality without using the original cover photo. The watermark capacity is increased by the proposed block-based SVD method, and the security level of the watermarked image is improved by the encryption technique. Future work aims to improve the capacity, watermark strength and quality of the reconstructed image against high levels of attack.

REFERENCES

1. Satendra Kumar, Ashwini Saini, Papendra Kumar, " SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform", IJCA,Vol. 45No. 10, pp.7-11, May 2012.
2. Makbol, N.M., Khoo, B.E.: Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. Int. J. Electron. Commun.(AEU) 67(2), pp. 102–112, 2013.
3. Ray, Arun Kumar, et al. "Development of a new algorithm based on SVD for image watermarking." Computational Vision and Robotics. Springer India, pp.79-87, 2015.
4. Sondes, Mohamed, and Abdellatif "Hybrid SVD- DWT watermarking technique using AES algorithm for medical image safe transfer" 16th international conference on Sciences and Techniques of Automatic control & computer engineering - STA'2015, Monastir, Tunisia, December 21-23, 2015
5. Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain. "National Academy Science Letters 37.4, pp. 351-358, 2014.
6. S. Murty, Dr. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme using Hybrid DWT-DCT-SVD Technique", IJCSNS,Vol.10,No.10, pp. 185-192, Oct 2010.
7. Zhou, Yaxun, and Wei Jin. "A novel image zero-watermarking scheme based on DWT-SVD." Multimedia Technology (ICMT), 2011 International Conference on.IEEE, pp. 2873-2876, 2011.
8. R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.
9. Chang, C.C., Tsai, P., Lin, C.C.: 'SVD-based digital image watermarking scheme', Pattern Recognit. Lett, 2005, 26, (10), pp. 1577–1586

ANTIOXIDANT PLASMA HIGH SERUM URIC ACID LEVELS IN DIABETES MELLITUS IN TYPE II

P Geetha Swarupa[1] ., V. Janki [2]

1 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ pgeetha@gmail.com)

2 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— The security and authentication of people is essential in many areas of our lives, and most people need to authenticate their identities on a daily basis. Examples include ATMs, secure building access, and international travel. Biometric identification offers a valid alternative to traditional authentication mechanisms such as ID cards and passwords, while overcoming many of the shortcomings of these methods. Iris recognition is more accurate than any other biometric feature. The goal of this project is to create a functional prototype program that acts as an iris recognition tool, comparing the RED (Ridge Edge Direction) and HWT (Hybrid Wavelet Transform) algorithms for feature extraction in order to implement iris authentication system implementations implemented in MATLAB to be more accurate and useful, which is simple is to use. Our main goal is to develop an application-based system that accurately authenticates everyone. The app-based system provides security for the door of a company or institute by repairing our system, which authenticates everyone and shows the result when the person is authenticated. The door will open automatically. We'll show it in the graphical user interface (GUI). Our goal is to provide the most accurate security system for everyday use.

Keywords* : *Diabetes Mellitus Type II; Serum Uric Acid; Antioxidant.

1. INTRODUCTION

The term diabetes mellitus (DM) describes a metabolic disorder of multiple etiologies, characterized by chronic hyperglycemia with disorders of the metabolism of carbohydrates, fats and proteins, which are due to defects in insulin secretion, the action of insulin, or both. The total number of people with diabetes is projected to increase from 171 million in 2000 to 366 million in 2030.1 Type II diabetes is a heterogeneous group of diseases characterized by insulin resistance, low insulin secretion, and increased glucose production. For example, in type II DM, hyperglycemia can lead to the production of reactive oxygen species (ROS). Superoxide, hydrogen peroxide and hydroxyl radicals during enzymatic or enzymatic pathways such as oxidative glucose phosphorylation, polyol pathway, advanced glycation end products, leakage during the mitochondrial respiratory chain and activation of nicotinamide adenine dinucleotide phosphate oxidase. Oxidative stress in type II DM and as a preventive measure, the body can increase its preventive antioxidants as a defense mechanism. Uric acid is the most abundant antioxidant found in plasma.3 Urate, the soluble form of uric acid in the blood, can scavenge superoxide radicals, hydroxyl radicals, and singlet oxygen, and also chelate transition metals.4 Recent researchers have shown that uric acid has extreme absorption properties.5 An increase in serum uric acid , also called hyperuricemia, is a condition that causes people to have higher levels of uric acid. Serum uric acid, especially more than 7.2 or 6.0 mg / dl, in adult men and women. The hyperuricemia associated with glycemia reflects the role of hyperglycemia in generating oxidative stress in patients with type II diabetes6. Therefore, uric acid can be estimated as a biochemical parameter to determine its relationship as an antioxidant in type II diabetes. This study was conducted to understand the relationship between serum uric acid levels in type II diabetes.

II. MATERIAL AND METHODS

A prospective, analytical, and case-control study, "A Study of Elevated Serum Uric Acid Levels in Type II Diabetes Mellitus", was conducted between January 2018 and January at the AcharyaVinoba Bhave Rural Hospital (AVBRH) in Sawangi, Meghe, Wardha. 2019. Approval from the university's ethics committee was obtained to conduct the study.

The patients who came to the central clinical laboratory of various outpatient services (OPD) of the AVBRH for the assessment of plasma glucose were selected. The informed consent of all patients for the blood tests was obtained. Name, age, gender, height and weight were recorded. Five ml of venous blood was collected from empty stomach and post-meal patients to assess parameters such as fasting

and post-meal blood sugar, glycated hemoglobin, and serum uric acid.

Parameter	Method of Estin
Plasma Glucose (Fasting and Post meal glucose)	GOD-POD meth
Glycated Hemoglobin (HbA1c)	Latex Agglutinat
Serum Uric acid	Uricase-PAP met

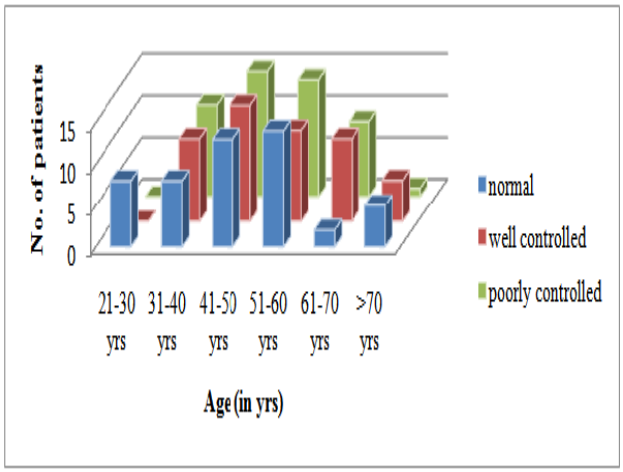
A total of 150 subjects were examined and divided into three groups according to their glycated hemoglobin level: -Group 1 (normal subjects): 50 patients with an HbA1c level <6%, Group 2 (well-controlled diabetes): 50 patients with an HbA1c level 6- 8% and group 3 (poorly controlled diabetes): 50 patients with an HbA1c level> 8%. The statistical data were expressed as the mean ± standard deviation. SPSS version 16 was carried out for statistical analysis. The Anova test was used for comparison between more than two groups and the Student t-test for comparison between two groups. A "p" value less than 0.05 was considered statistically significant.

III. RESULTS & DISCUSSIONS

This study found elevated serum uric acid levels in the poorly controlled group (7.12 ± 0.57) compared to the normal group (1.96 ± 0.52) and the well-controlled group (4.71 ± 0.57). 0.29), which is statistically very significant (<0.0001).

Table 1: Age-wise distribution

Age in years	Normal	Well controlled	Poorly controlled
21 - 30	8	0	0
31 - 40	8	10	11
41 - 50	13	14	15
51 - 60	14	11	14
61 - 70	2	10	9
> 70	5	5	1
Total	50	50	50



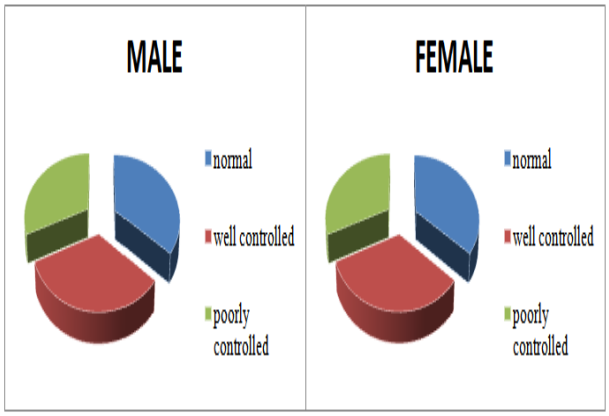


Figure 1: Sex-wise distribution of patients in study groups

Similar results were seen in several other studies. SudhindraRao M et al. Reported in 2012 that elevated serum uric acid levels are strongly linked to common health problems such as obesity, insulin resistance, metabolic syndrome, essential hypertension, and kidney disease. They found that higher serum uric acid levels in prediabetes than in controls and lower in diabetes mellitus than in prediabetes can serve as a possible economic biomarker for impaired glucose metabolism. According to Abbas Dehghan et al. A quarter of diabetes cases can be attributed to high serum uric acid levels. The recognition of elevated serum uric acid levels as a risk factor for diabetes has been the subject of debate for several decades as it is believed that hyperuricemia is a consequence of insulin resistance rather than its precursor, he concluded in a study by Butler R, et al. Hyperuricemia has been shown to be associated with obesity and insulin resistance, and therefore type II diabetes mellitus, which was reported by Idonije et al. Hyperuricemia induces endothelial

dysfunction that leads to nephropathy in patients with type II diabetes, and Tseng's study also shows that even mild hyperuricemia leads to kidney damage. Theuric acid is a very good diagnostic marker for detecting kidney damage in the early stages.

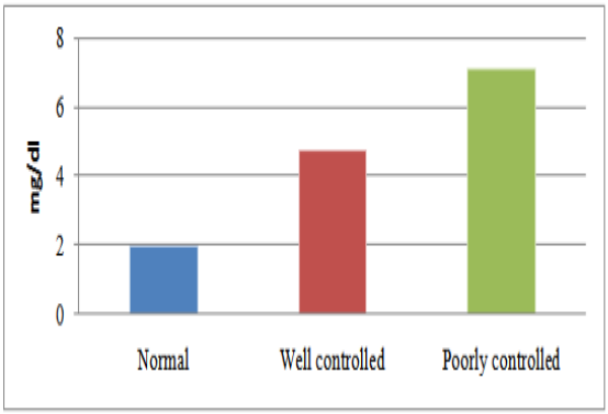


Figure 2: Serum uric acid values in study groups

IV. CONCLUSION

This study showed significantly increased serum uric acid (UA) levels in patients with type II diabetes compared to normal and well-controlled subjects. This is in line with some previous studies suggesting a possible association between UC levels and type II DM. Interestingly, DU is a risk factor for the development of metabolic, cardiovascular and kidney diseases in patients with type II diabetes mellitus. We conclude that the prevalence of hyperuricemia plays a key role in the progression of type II diabetes mellitus. However, given the possible association between increased serum uric acid and insulin resistance, glucose intolerance, and diabetes progression, more research is needed to determine whether it is effective to use UA levels as a predictor of preventing type II diabetes.

REFERRENCES

1. Abbas Dehghan, Mandy Van Hoek, Eric J. G. Sijbrands, et. al. “High Serum Uric Acid as a Novel Risk Factor for Type 2 Diabetes”. Diabetes Care, 2008; 31(2): 361–362.
2. Butler R, Morris AD, Belch JJ, Hill A, Struthers AD: Allopurinol normalizes endothelial dysfunction in type 2 diabetics with mild hypertension. Hypertension 35:746–751, 2000.
3. BO, Festus O, Oluba OM; Plasma Glucose, Creatinine and Urea levels in type 2 Diabetic patients attending a Nigerian teaching hospital. Research Journal of Med. Science, 2011; 5 (1) 1-3.
4. Tseng CH; Correlation of uric acid and urinary albumin excretion rate in patients with type 2DM inTaiwan. Kidney Int, 2005; 68: 796-801.
5. Wild S, Roglic G, Green A, Sicree R, King H. “Global Prevalence of Diabetes. Estimates for the year 2000 and projection for 2030”. Diabetes Care 2004; vol. 27: 1047–1053.
6. Forbes JM, Coughlan MT, Cooper ME, Oxidative stress as a major culprit in kidney disease in diabetes. Diabetes.2008;57(6):1446-54.
7. Tzounakas VL, Georgatzakou HT, Kriebardis AG, Papageorgiou EG, Stamoulis KE, Foudoulaki-Paparizos LE, et al. Uric acid variation among regular blood donors is indicative of red blood cell susceptibility to storage lesion markers: A new hypothesis tested. Transfusion. 2015;55(11):2659-71.
8. Simie MG, Jovanovich SV. Antioxidation mechanisms of uric acid. J Am Chem Soc. 1989;111:5778-82.
9. SudhindraRao M., Bino John Sahayo, “A Study Of Serum Uric Acid In Diabetes Mellitus And Prediabetes In A South Indian Tertiary Care Hospital”. NUJHS, 2012; Vol. 2(2): 18-22.
10. Zargari M, Allameh A, Sanati MH, Tiraihi T, Lavasani S, Emadyan O. Relationship between the clinical scoring and demyelination in central nervous system with total antioxidant capacity of plasma during experimental autoimmune encephalomyelitis development in mice. NeurosciLett. 2007;412(1):24-8.
11. Greene DA, Stevens MJ, Obrosova I, Feldman EL. Glucose induced oxidative stress and programmed cell death in diabetic neuropathy. Eur J Pharmacol. 1999;375(1-3):217-23.

ESTIMATE OF IONIZED CALCIUM AND INTRACELLULAR MAGNESIUM FOR ASSESSING PREECLAMPSIA

V. Janki [1] ., P Geetha Swarupa [2]

1 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ vjanaki12@gmail.com)

2 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract— Preeclampsia is a leading cause of morbidity and mortality in both maternal and fetal life (1). Although the etiology is unclear, recent studies suggest that magnesium and calcium levels may play a role in preeclampsia. The aim of this study was to determine the relationship between intracellular magnesium levels and ionized calcium levels in pregnancies with preeclampsia compared to normal pregnancies. Blood samples from 100 preeclampsia women and 30 controls were analyzed for intracellular magnesium levels (RBC) and ionized calcium levels. The outcome of the pregnancy was analyzed and compared in both groups. In this study, a significant decrease in intracellular magnesium was found in preeclampsia patients compared to normal pregnant women (p <0.05). In patients with preeclampsia, the intracellular magnesium is 5.21 mg / dl with a limit value of 6.36 mg / dl with a sensitivity of 99% and a specificity of 96.6%. The ionized calcium content in patients with preeclampsia is 1.42 mmol / l, with a limit value of 1.37 mmol / l, a sensitivity of 95% and a specificity of 98% (p <0.05). Intracellular magnesium is significantly decreased while ionized calcium increases in preeclampsia patients compared to normal pregnant women, suggesting the possible role of intracellular magnesium and ionized calcium in the physiology of the etiopathogenesis of hypertension during pregnancy. The estimate of ionized calcium is the simplest and cheapest parameter for assessing preeclampsia.

Keywords* : *Diabetes Mellitus Type II; Serum Uric Acid; Antioxidant.

1. INTRODUCTION

Hypertension is the second leading cause of maternal mortality and it is estimated that up to 30% of perinatal deaths are due to hypertensive pregnancy disorders. Preeclampsia is one of the most common causes of morbidity and mortality in both mothers and fetuses [2]. It is a systemic disease that affects about 5 to 7% of all pregnancies and is the most common but least understood pregnancy disorder [3]. It is a rapidly progressing disease characterized by high blood pressure, platelet aggregation, swelling of the lower extremities, and protein in the urine [4]. Sudden weight gain, headache, and blurred vision are the main symptoms. Typically, hypertension and preeclampsia occur by the end of the second or third trimester [5]. The pathophysiological mechanism is characterized by a failure of trophoblastic invasion of the spiral arteries, which may be associated with an increase in vascular resistance of the uterine artery and a decrease in placental perfusion [2]. The incidence in primigravid women is around 6% [6]. Clinically, preeclampsia is characterized by a constant increase in blood pressure above 140/90 mmHg, proteinuria and edema [7]. It can be associated with complications such as visual disturbances, oliguria, eclampsia, hemolysis, elevated liver enzymes, thrombocytopenia, pulmonary edema and growth retardation of the fetus [8]. Early detection and prompt management help reduce complications of this disease. Despite its prevalence and severity, the pathophysiology of this multisystem disorder is not yet well understood and its etiology is not yet fully understood [9]. Environmental and nutritional factors can influence the etiology of preeclampsia. Magnesium is the fourth common cation in the body required by the 300 enzyme system [10]. The decrease in intracellular Mg would lead to a partial depolarization of the membrane and a decrease in repolarization in connection with cell accumulation and possible cellular effects dependent on calcium [11, 12]. Calcium plays an important role in muscle contraction and in regulating the water balance of cells. The change in plasma calcium concentration leads to a change in blood pressure. Decreased serum calcium and increased cellular calcium can cause high blood pressure in mothers with preeclampsia. An increase in the cellular calcium concentration with decreasing serum calcium leads to a narrowing of the smooth

muscles in the blood vessels and an increased vascular resistance [13].

2. Materials and methods

The study was conducted in two groups that included 30 [n = 30] healthy pregnant women aged 20 to 30 years [controls] who were non-diabetic, non-hypertensive, and without kidney disease. Group 2 consists of 100 pregnant women [n = 100] aged 20 to 30 years with preeclampsia with edema BP140 / 90 mm hg. In these patients, blood pressure was normal for the first 20 weeks of pregnancy. No o / o HTN and previous kidney disease. All women in both groups were of the same gestational age (24-34 weeks). Methods 3 ml of venous blood is collected in a clean sterile vial, 2 ml of which is washed with normal saline, centrifuged, lysed and leveled. Intracellular magnesium is estimated using the Calmagite method, ionized calcium in serum is estimated using the ISE (ion-selective electrode) method.

3. Results

The mean intracellular magnesium value of group 2 [preeclampsia] is 5.21 mg / dl, group 1 [controls] is 6.3 mg / dl ($p < 0.05$). The mean value of ionized calcium in patients with preeclampsia is 1.42 mmol / l and in controls 1.31 mmol / l ($p < 0.05$) [Table 1]

Table:1

Groups	RBC Mg	Ionized Cal	P valie
Group -1 (Pre eclampsia)	5.21mg/dl	1.42mmol/L	0.05
Group-2 (control)	6.3mg/dl	1.31mmol/L	0.05

Table:2

Parameter	Cut off value	Sensitivity	Specificity	Diagnostic efficiency
RBC Mg	6.36mg/dl	99%	97%	98%
Ionized Calcium	1.37mmol/L	96%	95%	97%

The cut off value is calculated by taking the mean of controls and subtracting 2SD
Sensitivity = TP/TP+FNx100
Specificity= TN/FP+TNx100
Diagnostic Efficiency=TP+TN/Total no of pts evaluated
Table:2 suggests that the cut off value of RBC Mg is 6.36mg/dl, sensitivity is 99%, specificity is 97%, diagnostic efficiency is 98%. The cut off value of ionized calcium is 1.37mmols/L, sensitivity is 95%, Specificity is 95%, Diagnostic efficiency.

4. Discussion

Preeclampsia is a specific syndrome with decreased perfusion, secondary to vasospasm and endothelial activation with edema, BP-140/90 mm Hg, after 20 weeks of gestation and more often in the short term [14]. Magnesium acts as a calcium anthoganist via calcium channels, regulates energy transfer, stabilizes the membrane, Mg has a negative effect on the synapses and has been used as an anticonvulsant. The mechanism of action of synapses is related to the competition between calcium and Mg in the secretion of stimuli during the release of the transmitter. The presynaptic inhibition of acetylcholine release at the neuromuscular junction is best described. Its effect as an anticonvulsant is subordinate to the Mg antagonist at the level of methyl aspartate D (NMPA) receptors. Its stimulation is known to cause a post-synaptic potential (EPSP) excitability, which causes seizures. Mg has been used successfully as an anticonvulsant against eclampsia [15]. It has been shown experimentally that Mg blocks the NMDA subtype of the glutamate channel through which calcium enters the cell and causes neuronal damage in cerebral ischemia [10]. Ischemia leads to a decrease in transmembrane potential, which allows membrane phospholipids to affect calcium, which is hydrolyzed by activated enzymes. In addition to the outer lipid membrane, Magnesium blocks calcium at intracellular locations. Pathological findings in the brain of eclampsia patients show evidence of vasospasm; the finding was supported by cerebral angiography and computed tomography and is consistent with the findings in the vascular system [16].

5. Conclusion

In the present study, the level of intracellular magnesium decreases while ionized calcium increases. Ionized calcium can be considered a relatively better endpoint for assessing preeclampsia and eclampsia compared to Mg, since estimating Mg in red blood cells is a lengthy and tedious process. Patient samples can be sent to the biochemistry laboratory with an assessment of electrolytes, and ionized calcium can be estimated. Assessing ionized calcium can be helpful in preventing eclampsia that is harmful to patients.

REFERENCES

1. Ziael S, Ranjkesh F, Faghihzadeh S. Evaluation of 24-hour copper in pre-eclamptic vs normotensive pregnant and non-pregnant women. Int J Fertil Steril. 2008; 2:9–12.
2. Sarsam DS, Shamden M, Al Wazan R. Expectant versus aggressive management in severe pre-eclampsia remote from term. Sing Med J. 2008;49:698. [PubMed]
3. Akinloye O, Oyewale OJ, Oguntibeju OO. Evaluation of trace elements in pregnant women with pre-eclampsia. Afr J Biotechnol. 2010;9(32):5196–5202.
4. Cunningham FG, Leveno KJ, Bloom SL, Hauth JC, Gilstrap LC III, Wenstrom KD. Williams Obstetrics. 22nd ed. New York: McGraw – Hill; pp. 761–808.
5. Bringman J, Gibbs C, Ahokas R. Differences in serum calcium and magnesium between gravidas with severe pre-eclampsia and normotensive controls. Am J Obstet Gynecol. 2006;195:148.
6. Borzeix MG-Akimjak JP charles P.Lenfent M Cohn.R- Effect of magnesium on GABA inhibition induced convulsion in mice eds. Magnesium, London John Libbery 1995,177-180.(1993).
7. Classen HG Speich M,Schimats Chek,HF and Rattanatayaram W ibid.,13-20(1994).
8. F.Cunnigham, kennethleveno,Stevenbloom,Mc Graw Hill Professtional.WilliamA. Text book of Obstetrics, Edition22,Sec Vll,pg,763-765,(2005).
9. The Eclampsia trail collaborative group.Which anti convulant for woman with preeclampsia. Evidence from the collaborative eclampsia trial.Lancet,345,1455-63.(1995).

ISOLATION AND PARAMETER OF ESCHERICHIA COLI IN RURAL AREAS

K. Amitha[1] ., V. Janki [2]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ kamitha112@gmail.com)

2 Associate Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract* : *Isolation and characterization of E. coli in fast foods concerns due to their presence indicates fecal contamination of the food. To identify, characterize and RFLP pattern analysis of E. coli isolated from vended fast foods in rural areas of Delhi-NCR. Genomic DNA was used to perform RFLP pattern analysis. Eighteen out of 24 (75%) analyzed samples of fast foods had E. coli contamination. The highest number of E. coli was isolated from chicken biryani and golgappa (83.33 %) and burger and vegetables ready to eat fast food (66.66 %) samples were also significantly E. coli positive. RFLP profiling of E. coli isolates was observed..

Keywords* : *Vended fast foods, Escherichia coli, Genomic DNA, RFLP profiling.

1. INTRODUCTION

Food safety is an essential component of public health, linking health to different food production and agriculture sectors1. Most common bacterial pathogen is Escherichia coli which is capable of causing intestinal disease. Some E. coli are nontoxic and are found naturally in the intestine of humans2. Escherichia coli strain O157 is a part of enterohemorrhagic Escherichia coli and has been identified as the cause of numerous outbreaks by causing, hemorrhagic colitis, hemolytic uremic syndrome, diarrhea3. In developing countries street food and junk food plays an important role4. Food sector has experienced important growth during the earlier period because of social and economic changes in developing countries. They give food to large number of people daily with an extensive range of ready-to-eat foods and sometimes prepared these foods in the public places or streets, reasonably low-priced and easily offered5. Safe water for food and human consumption is important, but there is a limited supply. Developing countries has water shortages during summer season in many colonies and depends on other sources of water including boreholes and water tankers. Microbiological assessment of drinking water and food is important to reduce exposure to cause intestinal disease6. A food borne pathogen E. coli O157:H7 was first recognized in America7 after an occurrence of hemorrhagic colitis following the ingestion of undercooked hamburgers at a fast-food restaurant chain8. The present research work in rural areas represents the data of E. coli in fast food products. Mostly microorganism present in different types of food items is non-toxic9. So it is very important to identify the toxic pathogen in order to build up an appropriate test to detect pathogen. Culturing technique is a conventional method to identify food born pathogen by plating to isolate pure culture. Genomic DNA isolation technique can arrange within pool culture of bacteria. Food borne pathogen along with dissimilar bacterial species can detect by RFLP technique. The main objective of this work was to find out the presence of E. coli in many street fast food or ready to eat food samples in rural areas in Delhi-NCR.

II. Materials and Methods

Sample collection: Approximately 100 g of each 24 samples of street fast food of 4 categories (6 samples of chicken biryani, 6 samples of burger, 6 samples golgappa and 6 samples of vegetables) were collected between July 2018 and August 2018 from different places in rural areas of Delhi-NCR. All samples were tested within 24 h of collection. Ten grams of each food sample was mixed with one eighth strength Ringers Solution. The sample was homogenized with an electric hand blender at 5000 rpm for 10-12 minutes (10-1 dilution), followed by serial dilutions up to 10-6 dilution.
Isolation and test of E. coli: The most probable number (MPN) method was used for determining E. coli counts 10,11. Fermentation tubes (10 ml) of lauryl tryptose broth medium were poured with different concentration. The tubes were inoculated with 5 ml, 1 ml with 5 ml, and 1 ml and 0.1 ml amount of sample and incubated at 37°C for 24 h. All tubes under experiment producing gas after 24 h of incubation, was further tested

for conformation. In this analysis, dilutions of the each sample were made using peptone water. 1ml of each sample was pipetted into one sterile test-tube containing 9 ml of peptone water, making 1:10 dilution, secondtest-tube making 1:100 dilution and third test-tube making 1:1000 dilution respectively. From all the three dilutions, 1ml was transferred into already prepared Mac Conkey Broth containing each 9 ml (triplicate) with inverted positioned Durham's tubes. The tubes were covered with cotton wool and incubated at 37°C for 24 hours. A very minute quantity from each culture showing production of acid and gas was transferred to Brilliant Green Bile Broth (Oxoid) and incubated for 48 h at 37°C and 44.5°C. Streaking on the eosine methylene blue (EMB) agar plate was done for further confirmation that was performed10. One or more plates containing EMB agar medium were streaked from presumptive positive test tubes in such a way that discrete colonies may appear. The plates were incubated at 37°C for 24 h. Typical nucleated colonies with or without metallic sheen indicates positive results. Few suspected E. coli colonies from each sample were selected. Further biochemical tests were done for the identification of Escherichia coli according to 12. IMViC test was performed to distinguish between E. coli and Enterobacter aerogenes 10. Two isolates identified as E. coli were further characterized based on DNA polymorphism by RFLP.

III. Results

100 g of each 24 samples of street fast food of 4 categories (6 samples of chicken biryani, 6 samples of burger, 6 samples golgappa and 6 samples of vegetables).

Fig. 1. Agarose gel electrophoresis pattern of the extracted DNA

E. coli was isolated from 18 out of 24 (75%) food samples analyzed in this study; no E. coli isolates were obtained from the remaining 6 samples. E. coli was detected in 5 out of 6 (83.33%) chicken biryani and golgappa samples and in 4 out of 6 (66.66 %) samples of burger and vegetables ready to eat foods. Genomic DNA extracted from E. coli samples collected in this research work. The A260 value of two DNA sample was 1.8296 and 1.7887. The A260/A280 ratio was 1.954 and 1.846 respectively. Some alterations in the phenol/chloroform method were done in this work. These were the addition of brine solution and ice cold isopropanol before phenol: chloroform extraction of samples. Above given two steps enhanced the yield of high-quantity and high-quality genomic DNA and was agreeable to further molecular characterization with RFLP. The reliability of the extracted DNA and restriction fragment pattern was analyzed by agarose gel electrophoresis (Figs. 1). Most digested DNA fragments size was in the range from 300 to 3000 bp (Fig. 2). A powerful marker for molecular finding of pathogenic organism is RFLP digestion pattern. PCR amplification of the gene with the suitable primer would be specific for particular organism. In future, the specific gene of E. coli may be amplified and sequencing of the gene could expose the improved consideration of pathogenicity.

IV. DISCUSSION

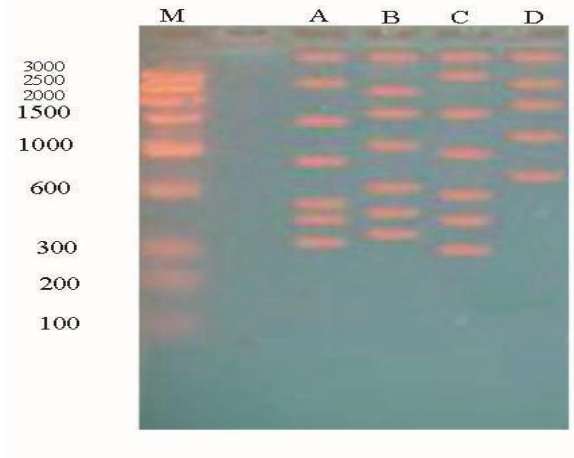


Fig. 2. RFLP profiling of sample after electrophoresis

In this research work 75% food sample found as E. coli positive. The frequency of E. coli was found to be highest in chicken biryani and golgappa. E. coli was most frequently detected

in convenient foods and 50% samples were found to be E. coli contaminated14. Presence of E. coli in food may indicate fecal contamination which might be due to insufficient cooking, use of raw vegetables, cross contamination between raw and cooked food and contaminated ingredients15. So, presence of E. coli in 75% ready to eat food samples in the present study might be representing fecal contamination. People who depend on such food are often more interested in its convenience than in questions of its safety, quality and hygiene. Pathogenic bacteria including S. aureus, E. coli and Salmonella in restaurants would transfer to the cooked foods by contaminated staffs' hands or dishes16. Total E.coli was found to be present in all samples, indicating an alarming situation of health hazard. Many rural areas are endemic zone for diarrhoeal diseases every year, more than 3 % of death of children below 6 years of age is attributed to diarrhea.

V. CONCLUSION

Ready to eat foods vended in street fast foods in rural areas in Delhi NCR had unacceptable levels of contamination with E. coli. Unhygienic practice may represent the risk factors connected with contamination of packed food. Food-borne disease is an urgent public health problem and needs search association. RFLP pattern analysis might be useful for molecular recognition of pathogenic organism among different species if coupled with PCR.

REFERENCES

1. N. Barro, P. Nikiéma, CAT. Ouattara, A. S. Traoré. Evaluation de l'hygiène et de la qualité microbiologique de quelques aliments rue et les caractéristiques des consommateurs dans les villes de Ouagadougou et de Bobo-Dioulasso, Rev Sci Tec Sci Santé, 25, 7-21. 2002.
2. T. S. Thani, S. M. L. Symekher, H. Boga and J. Oundo, Isolation and characterization of Escherichia coli pathotypes and factors associated with well and boreholes water contamination in Mombasa County, Pan Afr Med J, 23: 12, 2016.
3. L. W. Riley, R. S. Remis, S. D. Helgerson, H. B. McGee, J. G. Wells, B. R. Davis, R. J. Hebert, E. S. Olcott, L. M. Johnson, N. T. Hargrett, P. A. Blake, and M. L. Cohen. Hemorrhagic colitis associated with a rare Escherichia coli serotype, N. Engl. J. Med, 308:681–685, 1983.
4. J. P. Nataro and J. B. Kaper. Diarrheagenic Escherichia coli, Clin. Microbiol. Rev., 11:142–201, 1998.
5. S.H. Kumar, K. Iddya, I. Karunasagar, Molecular methods for rapid and specific detection of pathogens in seafood, Aquacult Asia, 3, 34-37, 2002.
6. J.G. Cappuccino, N. Shermam Microbiology: A Laboratory Manual. Fourth the Benjamin/Cummins Publishing Company Inc California USA, 1999.
7. J.P. Harley, L.M. Prescott, Laboratory Exercises in Microbiology, Fifth Edition, The McGraw−Hill Companies, 2002.
8. M.B. Coyle, J.A. Morello, P.B. Smith, Aerobic bacteria. In: Lennette EH, Balow A, Housler WJ, Shadomy HJ (eds) Manual of Clinical Microbiology, American Society for Microbiology, Washington DC, USA, 143-411, 1985.
9. B. Neumann, A. Pospiech, H.U. Schairrer, Rapid isolation of genomic DNA from Gram-negative bacteria, Trends Genet 8, 332–333, 1992.

ANTIBACTERIAL & ANTIOXIDANT PROPERTIES OF METHANOLIC EXTRACT FROM ARTOCARPUS LEAVES AND STEM BARK FOR USE AS A PEELABLE MASK

K. Amitha [1] ., Dr. P Geetha Swarupa [2]

1 Assistant Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India, (✉ vjanaki12@gmail.com)

2 Professor, Department of H&S., Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India

Abstract* : *Antibacterial and antioxidant activities were carried out using a methanolic extract from Artocarpus leaves and stem bark for use as a peelable mask. The raw material was macerated with methanol and the resulting filtrate was evaporated until the concentrated raw extract was obtained. The crude extract is tested using various tests such as: B. phytochemical screening, antibacterial test for Propionibacterium acnes and Staphylococcus aureus with an extract concentration of 50; 100; 150 and 200 ppm and antioxidant test according to the DPPH method. The additional test was performed to evaluate the characteristics of the peelable mask such as homogeneity, pH, organoleptic and irritation test. The result of the photochemical screening showed that these extracts were dominated by tannins and saponins. The antibacterial test against P. acnes showed that the leaf extract with concentrations of 50, 100, 150 and 200 ppm had the zone of inhibition 9.6; 9.9; 10.4 and 11.3 mm. The other extract, the stem bark extract, provided the zone of inhibition 8, 4; 8.8; 9.5 and 10.5 mm with a similar extract concentration. These data showed that the antioxidant activity of the parent bark extract greater is than that of the stem bark extract. The clinical tests of the anti-stick mask formulation showed that F1, F2 and F3 are of good homogeneity and that the pH was 6.7; 6.7 and 5.8. The irritation test showed a negative result for all formulations.

Keywords* : *Antibacterial, Antioxidant, P. Acnes, S. Aureus, Jackfruit.

1. INTRODUCTION

The problem with which you faced in the medical field today is , is bacterial resistance to antibiotics in developed and developing countries. Much research has therefore focused on the production of antibiotics from the synthesis process and secondary metabolites of natural substances to cope with bacterial resistance [1]. Bacteria are microorganisms that cannot be seen with the naked eye, but only under a microscope. Among them are the bacteria Staphylococcus aureus and Propionibacterium acnes. Staphylococcus aureus is a coconut-shaped bacterium with a diameter of about 1 µm that is arranged in irregular groups [2]. In humans, Staphylococcus aureus occurs in the nose, skin, throat, and others. These bacteria can cause various infections, including pneumonia, meningitis, empyema, endocarditis, pimples, pyoderma, or impetigo [3] [4]. Propionibacterium acnes is a gram-positive bacterium and normal skin flora that play a role in the formation of acne [5]. Propionibacterium acnes secretes hydrolytic enzymes that damage polysebaceous follicles and produce lipase, hyaluronidase, protease, lecithinase and neurimidase, which play an important role in the inflammatory process [6]. One type of natural product that people use primarily to treat all kinds of health problems, including infections caused by bacteria, is jackfruit (Artocarpus heterophyllus Lam.) Jackfruit leaf contains flavonoids, saponins, and tannins that can act as antimicrobial agents. and induce the production of new skin cells [7]. In addition, the bark of the jackfruit stem contains secondary metabolites such as morin, sianoma clurin, flavonoids and tannins. New compounds were discovered especially for the flavonoid in the bark of the jackfruit stem, such as Morusin, Artonin E, Artocarpine, Cycloartobiloxanthone and Artonol B. The bioactivity of flavonoid compounds can be used as cancer, anti-inflammatory, diuretic and diuretic lowering blood pressure [8].

2. M ATERIALS AND METHODS

Leaf and stem bark of jackfruit (Artocarpus heterophyllus Lam) were obtained from Sigambal, Sumatera Utara. FeCl3.6H2O, CeSO4.4H2O, H2SO4 96%, DPPHwas obtained from Sigma Aldrich. Ethanol and methanol were obtained from Merck. All chemicals were used without further treatment.

Phytochemical evidence

Alkaloid test: the methanol extract from jackfruit leaves and stem bark was placed in

several test tubes. The tube was loaded with Wagner's reagent, the formation of a red / brown precipitate indicates the presence of alkaloids. Tube II was poured with Mayer reagent, the formation of a yellow precipitate indicates the presence of alkaloids. Tube III was penetrated with boucahardate reagent, the formation of a chocolate colored precipitate indicates the presence of alkaloids, and tube IV was deposited with Dragendorf's reagent, the formation of a red precipitate indicates the presence of alkaloids. Presence of alkaloids.

Flavonoid test: A methanol extract from jackfruit leaf and bark was placed in 2 test tubes. Tube I was loaded with 10% NaOH. If a blue-purple solution forms, it is positive for flavonoids. Concentrated HCl and Mg powder were added to tube II. If an orange solution forms, it is positive for flavonoids.

Terpenoid test: the methanol extract from jackfruit leaves and stem bark was placed in a test tube, then 1% CeSO4 in 10% H2SO4 was added. If a brownish-red precipitate has formed, it is certain that it contains terpenoids.

Tannin test: the extracts were treated with 3-4 drops of a ferric chloride solution. The formation of a bluish-black color indicates the presence of phenols.

Saponin test: 0 , 5 g of extract were stirred with 2 ml water. If the foam produced ten minutes long stops, this indicates the presence of saponins.

Table – 1: Mask Formulation from Jackfruit Leaf Methanol Extract

Ingredient	Concentration (g)		
	F_1	F_2	F_3
PVA	14	-	-
HPMC	-	2	-
Gelatin	-	-	30
Glycerin	5	5	5
Nipagin	0,2	0,2	0,2
Alcohol 96%	12,5	12,5	12,5
Aquadest	100	100	100
Extract	0,5	0,5	0,5

Jackfruit Leaf Methanol Extract Mask Review

Organoleptic: This observation included observations of color, odor, and clarity.

Homogeneity: The prepared gel was applied to the glass of the object, then the glass was clamped with another glass of the object. Homogeneity was observed with the naked eye.

Spreading test: The prepared gel was weighed 1 gram, then placed on a glass with a size of 20 × 20 cm, then covered with mica and weighed, after 1 minute the diameter was measured.

PH test: A total of 1 g of the gel produced was dissolved with 10 ml of Aquadest. The electrode of the pH meter was immersed in the gel solution and the resulting pH was recorded.

Drying Speed Test *:* The prepared gel mask was applied to the skin on the back of the hand, then the drying speed was measured to form a separation layer of the gel phase using a stopwatch.

Test of *irritation:* The test of *irritation* was carried out in the left hand of a panelist on 10 test subjects using the prepared gel (F tested 1, F2 and F3).

III. RESULTS AND DISCUSSION

Table - 2 Result of the phytochemical detection test Component of jackfruit leaves and bark
(+) positive (-) negative

The results of the phytochemical screening tests of jackfruit leaf and bark performed with the reagents Bouchardat, Meyer and Dragondrof (Table 2) showed no change in color, indicating that it was negative for the alkaloid. The terpenoid test results with 1% CeSO 4 did not form a brownish- red precipitate, so that the results were negative. Jackfruit leaves and bark contained saponins in the presence of foam when the extract was shaken. When the extract with 5% FeCl 3 tested was a blackish blue solution was obtained, indicating a positive result for tannin.

Table – 2: Result of Phytochemical Constituen Screening Test of Leave and Bark of Jackfruit

No	Test	Reagent	Leaves	Stem bark
1	Flavonoid	$FeCl_3$ 5%	-	-
		NaOH 10%	-	-
		H_2SO_4	-	-
2	Alkaloid	Bouchardat	-	+
		Dragendorf	-	-
		Meyer	-	-
3	Terpenoid	CeSO4 1%	-	-
		Salkowsky	-	+
4	Steroid	CeSO4 1%	-	-
		Salkowsky	-	-
5	Tanin	$FeCl_3$ 5%	+	+
6	Saponin	Aquadest	+	+

The results of the research are shown in Table 4. Jackfruit leaf extract can effectively inhibit bacterial growth at a concentration of 50 ppm. This shows that jackfruit leaf extract inhibits the growth of the bacterial colonies Propionibacterium Acnes and Staphylococcus aureus more effectively than jackfruit extract with the bacteria Propionibacterium Acnes and Staphylococcus aureus. In this study, a test was carried out for the antibacterial activity of jackfruit leaves and bark. Jackfruit leaves and bark were tested against Propionibacterium Acnes and Staphylococcus aureus. Phytochemical screening of jackfruit leaves and bark revealed tannins and saponins. Among the compounds detected, one of them was effective as an antibacterial agent [9] [10].

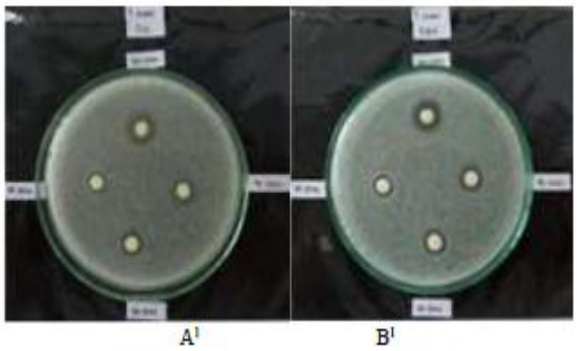


Fig. 1: Inhibitory Zones of Jackfruit Leaf Methanol Extract

The tannin contained in the leaf and stem of jackfruit bark is an active antibacterial compound that can inhibit the function of the cytoplasmic membrane in bacteria. At low concentrations, these compounds can also damage the cytoplasmic membrane and cause the release of important metabolites that activate the bacterial enzyme system, while at high concentrations they can precipitate cellular proteins. [Eleven]. Microorganisms react differently to the materials from which they were erased. There are differences between the species depending on the water content and pH of the environment and the age of the cell or spore, etc. Destruction or exponential destruction depends not only on the type of organism but also on different environmental conditions [12].

CONCLUSION

From the results of the research we can conclude:

1) According to a phytochemical screening test, jackfruit leaf and bark extract contained compounds of tannin and saponin.

2) The results of the antioxidant activity tests of the methanolic extract of jackfruit leaves and bark bark showed a strong anti-oxidation activity of 52 , 08 mg / ml and 33 respectively , 93 mg / ml.

3) The higher the concentration of methanolic extract from jackfruit leaves and bark, the greater the inhibitory effect on the growth of the bacteria Propionibacterium Acnes with inhibition zones of 9.6 to 11.3 mm at a concentration of 50 to 200 ppm and Staphylococcus aureus at Concentrations of 50-200 ppm with zones. Inhibition 6 , 2 - 9.2 mm

4) Methanol jackfruit leaf extract has better inhibitory effect on Propioni Acnes bacteria than methanol jackfruit extract, and methanol jackfruit leaf extract has better inhibitory effect on Staphylococcus aureus than methanolic jackfruit bark extract.

REFERENCES

1. Satish, S., Raghavendra, M. P. & Raveesha, K. A. (2008). Evaluation of the antimicrobial potential of some plants against human pathogenic bacteria. Advances in Biological Research, 2, 44.
2. Ibironke AA, Comparative study of the chemical composition and mineral element content of Artocarpus heterophyllus and Treculia africana seeds and seed oils. Bioresour Technol, 99: 5125-5129, (2008).
3. Jagtap UB, Bapat VA (2010). Artocarpus: A review of traditional uses, phytochemistry and pharmacology. J. Ethnopharmacol. 129:142-166.
4. Khan MR, Omoloso AD, Kihara M (2003). Antibacterial activity of Artocarpus heterophyllus. Fitoter 74:501–505.
5. Ríos JL, Recio MC (2005). Medicinal plants and antimicrobial activity. J. Ethnopharmacol. 100:80-84.
6. Reveny, J., Surjanto, J.T., & Lois, C. Formulation of Aloe Juice (Aloe vera (L) Burm. f.) Sheet Mask as Anti- Aging. 2016., International Journal of PharmTech Research, 9(7), 105-111
7. Paithanker, V. V. 2010. Formulation and evaluation of herbal cosmetic preparation using safed musli. International Journal of PharmTech Research, 2(4), 2261-2264.