ISSN:0975-9646

A New Hybrid Cloud Based Email Security Model Using Image Sequence Authentication, Compression and Cryptography

Ms. Nikita Rathi[#1], Mr. Prateek Nahar[#2], Mr. Vijay Kumar Verma[#3]

Department of Computer Science,
Rajiv Gandhi Proudyogiki Vishwavidyalaya
Airport Bypass Road, Gandhi Nagar, Bhopal,
Madhya Pradesh, 462036, India

Abstract— **Cloud computing one of the leading technologies in the market at difference places. Its capabilities are very useful to enhance the usefulness's we can see that Emails are commonly used way of communication and also sharing documents for businesses and individuals. Email service providers have taken several steps to meet the ever increasing security requirements but still struggling to find the best solutions for the problem. As Email service providers are taking advantages of the cloud service we also must take cloud security controls and try to find some optimize solution for the same. In this work we are proposing a new Email security model which is the combination of Image based authentication method, encryption and compression. We are trying to get the maximum benefit out of them, although they have the best results at their own area but we are trying to put a joint effort and trying to overcome the existing problem in the Email security.**

Keywords— **Cloud, Emails, Attacks, Image Authentication, Compression; Encryption.**

I. INTRODUCTION

Cloud computing has turned into an important technology where cloud services providers give computing resources to their customers (tenants) to host their data or perform their computing tasks. Distributed computing can be categorized into different administration deliver models, for example, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). [1] Virtualization is one of the key technologies utilized as a part of the IaaS cloud infrastructures. For instance, virtualization is utilized by a portion of the significant cloud administration providers, for example, Amazon and Microsoft in the procurement of cloud services. Email services by providers is commonly used from the organizations and individuals. Emails always had vulnerability issues because of its excessive use and confidentiality and authenticity of the data into the Email systems. In this work we want to address some of the major security issues inside the Email services by cloud platforms. Traditional security models are not enough for the Email service deployed at cloud and cannot meet the requirements of the consumers that we are trying to incorporate the successful approaches extracted from the history as far as access control and security in concern, and get a complete security solution that can give optimized and desired results. [1]

We will utilize the term tenant to allude to cloud customers who wish to access services from cloud providers. Tenants can themselves be utilizing their virtual machines to give services to their own customers; we will allude to customers (or users) as those who utilize the services of the tenants. Henceforth customers in our architecture are the customers of the tenants. All in all, the tenants in the cloud can run different operating systems and applications in their virtual machines. As the operating systems and applications of the tenants can be potentially expensive and complex, they may contain security vulnerabilities. Furthermore, there can be a few tenants on the same physical platform sharing resources in a cloud applications can be potentially exploited by an attacker to generate different types of attacks. These attacks can be targeted against the cloud infrastructure as well as against other virtual machines having a place with other tenants. So there is a need to design security architecture and create techniques that can be utilized by the cloud administration supplier for securing its infrastructure and tenant virtual machines. [2]

However there are a few issues that emerge when creating security as an administration for cloud infrastructures. In the current environment, the cloud administration providers don't for the most part offer security as an administration to their tenants. Case in point, in Amazon mentions that security of tenant virtual machines is the responsibility of the tenants since they are allowed to run any of the operating systems or applications1 (though it claims to secure the basic infrastructure). Thus tenants need to make their own particular arrangements for securing their virtual machines that are hosted in the cloud. Although tenants can utilize different security tools, for example, anti-virus and host based intrusion detection systems to secure their virtual machines, the limitations emerge because of these tools dwelling in the same system as the one being monitored and thus are defenseless against attacks. Likewise exactly tenants may not be fit for securing their tenant virtual machines. Henceforth there is a requirement for the cloud administration supplier to offer security as an administration to such tenants. [2]

At the present universe of networking system, Cloud computing is one the most important and creating concept for both the developers and the users. Persons who are interrelated with the networking environment, distributed computing is a best platform for them. Therefore in recent days giving security has turned into a significant testing issue in distributed computing.

In the cloud environment, resources are imparted among the majority of the servers, users and individuals. As a result files or data stored in the cloud get to be interested in all. Therefore, data or files of an individual can be taken care of by all other users of the cloud. Thus the data or files get to be more helpless against attack. As a result it is easy for an intruder to access, abuse and destroy the first type of data. An intruder can likewise interrupt the communication. In addition, cloud administration providers give different types of applications which are of extremely critical nature. Henceforth, it is extremely essential for the cloud to be secure. Another issue with the cloud system is that an individual might not have control over the spot where the data expected to be stored. A cloud client has to utilize the asset allocation and scheduling, gave by the cloud administration supplier. Thus, it is likewise important to protect the data or files in the midst of unsecured processing. Keeping in mind the end goal to take care of this issue we have to apply security in distributed computing platforms. In our proposed security model we have tried to take into account the different security breaches as much as conceivable. [2]

At present, in the range of distributed computing different security models and algorithms are connected. But, these models have neglected to unravel all most all the security threats. Also for E-commerce and different types of online business, we have to infer high capacity security models in distributed computing fields. Security models that are created and currently utilized as a part of the distributed computing environments are chiefly utilized for giving security to a record and not for the communication system. Additionally present security models are sometimes uses secured channel for communication. But, this is not cost effective procedure. Once more, it is uncommon to discover a joined work of principle server security, transaction between them et cetera. A few models attempt on talking about these, but are completely dependent on client approach. The models typically neglect to utilize machine intelligence for generating key and more current proposed model. A few models have proposed about equipment encryption system for secured communication system. The thought is normally straightforward, but the implementation is relatively difficult.

II. BACKGROUND

Various research on security in distributed computing has as of now been proposed and done in recent times. Identification based distributed computing security model have been worked out by different researchers. But just identifying the actual client does not all the time prevent data hacking or data intruding in the database of cloud environment. It is additionally an identification based work. The defect in this system is that it doesn't guarantee security in entire distributed computing platform. Research related to guaranteeing security in entire distributed computing environments was at that point worked out in different structures and formed. AES based file encryption system is utilized as a part of some of these models. But these models keep both the encryption key and encrypted file in one database server. One and only fruitful malicious attack in the server may open the entire information files to the hacker, which is not attractive. Some other models and secured architectures are proposed for guaranteeing security in distributed computing environment. Although these models guarantees secured communication between users and servers, but they don't encrypt the stacked information. For best security guaranteeing process, the uploaded information needs to be encrypted so none can think about the information and its location. Recently some other secured models for distributed computing environment are likewise being researched. But, these models additionally neglect to guarantee all criteria of distributed computing security issues.

- ***Image Authentication***

Image based authentication is included to provide additional security. With IBA, when the user performs first time registration on a website, he makes a choice of several secret categories of images that are easy to remember, such as pictures of natural scenery, automobiles. Every time the user logs in, a grid of randomly generated images is presented to the user. The user identifies images that were previously selected. Hash code is generated by the selected images, making the authentication process more secure than using only a static text password. It’s significantly easier and advantageous for the user because he has to remember [5]

The above paper will focus on the email protection against the various attack as we know that email consist of two parts the header part and the body part when an email get composed the .eml file get created that file is send to receiver end so first that file will get compressed by the compression algorithm i.e. loss less compression in which no loss of data take place after compression and the decompression. After that an encryption will be done so intruder can’t access the email content.

- ***Compression***

Huffman coding is an entropy encoding algorithm utilized for lossless data compression as a part of computer science and information theory. The term alludes to the utilization of a variable-length code table for encoding a source symbol, (for example, a character in a file) where the variable-length code table has been inferred in a particular manner based on the estimated probability of event for every conceivable estimation of the source symbol. Huffman coding uses a particular method for picking the representation for every symbol, resulting in a prefix-free code (that is, the bit string representing some particular symbol is never a prefix of the bit string representing whatever other symbol) that communicates the most well-known characters utilizing shorter strings of bits than are utilized for less regular source symbols. Huffman was ready to design the most efficient compression method of this type: no other mapping of individual source symbols to exceptional strings of bits will deliver a littler normal output size when the actual symbol frequencies concur with those used to create the code. A method was later found to do this in straight time if input probabilities (otherwise called weights) are sorted. [6]

- ***Advanced Encryption Standard (AES)***

Advanced Encryption Standard (AES) also known as the Rijndael algorithm is a symmetric block cipher [3]. It was recognized that DES was not secure because of advancement in computer processing power. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies [1]. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices [5]. AES has been tested for many security applications. After the encryption email will be become more secure due to this better level of authentication can be provided. [7]

III. Literature Survey

To ensure confidentiality or privacy and to make reliability on storage data at third place no of mechanisms are proposed by different researchers.

In the work [3] they presented a new novel authentication scheme is a combination of text passwords and graphical passwords for access control. First round of graphical authentication is a recognition based technique whereas second round of graphical authentication is a recall based technique. So they have used the term ‘hybrid’ to denote for user authentication than existing text-based password and graphical password methods for authenticated entry in the system. A necessary next step is a behavioural study of user, best practice says that both a lab study and a field study leveraging our real-world deployment of the system they adopted for security enhancement. The approach can be very useful for highly secured systems in the real life. Scheme they proposed will provide the following advantages:

- Users’ current sign-in experience is partially preserved.
- A text password alone which is stolen (e.g., by phishing or any other means) does not compromise an account.
- Random order of images in round-1 authentication provides a resistance to the shoulder surfing attacks.
- Password space is very large.
- It can be implemented in software alone, increasing the potential for large-scale adoption on the internet.

In this paper [4], they have proposed a new Implicit Password Authentication System where the authentication information is implicitly presented to the user. If the user “clicks” the same grid-of-interest compared with the server entries provided, consumer and user is implicitly authenticated for using the services of the system. No password information is exchanged between the client and the server in IPAS. Since the authentication information is conveyed implicitly, IPAS can tolerate shoulder-surfing and screen dump attack, which none of the existing schemes can absorb. Main advantage of IPAS is in creating a good authentication space with a sufficiently large collection of images to avoid short repeating cycles. Thus, a variation to the traditional login authentication scheme, viz. the new graphical scheme for authorization was introduced in their contribution. They introduce a framework of our proposed (IPAS) Implicit Password Authentication System is strong enough against the common attacks suffered by other authentication schemes.

In this work [5] they introduce an intriguing new primitive that they call Message-Locked Encryption (MLE). An MLE scheme is a symmetric encryption scheme in which the key used for encryption and decryption is derived from the message itself, which is provided for communication. Versions of this primitive are seeing widespread deployment and application for the purpose of secure communication, but in the absence of a theoretical concepts, they could not have a precise indication of what these methods do or do not accomplish. They investigate four MLE schemes and approaches, two of them are corresponding to in-use schemes and two new schemes.

In this work [6], they demonstrate that compression models perform very well for spam filtering, consistently outperforming established spam filters and other methods proposed in previous studies. They also show that compression models are very robust to the type of noise introduced in the text by typical obfuscation tactics used by spammers. This should make them difficult for spammers to defeat, but also makes them attractive for other text categorization problems that contain noisy data, such as classification of text extracted with optical character recognition. The large memory requirements of compression models are a major disadvantage of this approach. To this end, effective pruning strategies should be investigated in order to bring the models within limits that would be suitable for practical applications of the system. They also discussed about compression models actually be employed in practice, the adversarial nature of spam filtering suggests spammers will react to these techniques. It remains to be seen whether their efforts could reduce the long-term efficacy of the proposed approach.

In this paper [7], they address the open problem of characterizing what encryption via a random order-preserving function (ROPF) leaks about underlying data. They tried to put light over that, for a database of randomly distributed plaintexts and appropriate choice of parameters, ROPF encryption leaks neither the precise value of any plaintext nor the precise distance between any two of them from the available. They produce efficient new techniques. Revisited security of symmetric order-preserving schemes defined. They formally clarify the strengths and limitations of any OPE scheme proven to be a pseudorandom order-preserving function (POPF), and in particular, the efficient OPE scheme proposed in this paper. Basically for any POPF-secure OPE their analysis together with the result of provides upper bounds on the advantages of any adversaries attacking the one-wayness and distance one-wayness.

In this paper [8], they propose a joint compression and encryption algorithms resolve two major issues such as speed and security when confidential video data is sent over the network. In this study, comparative study of two categories of encryption algorithms viz. independent encryption algorithms and joint compression and encryption algorithms. The study shows that the joint compression and encryption algorithms are more secured and faster than all existing independent encryption algorithms. Compression and encryption algorithms can be classified into two main categories: Independent encryption technique and joint compression and methods of cryptography. Modified encryption techniques can further be classified as heavy weight and light weight encryption algorithms and also showing efficiency against the vulnerabilities. There are many algorithms available in the joint compression and encryption technique. Comparative study of the above mentioned algorithms is done in this study.

In this work [9], they designed Bi-serial DNA encryption algorithm containing technologies of DNA synthesis, PCR amplification, DNA digital coding, XOR operation as well as traditional cryptography and analysis. In the proposed PCR two primer pairs was used as the key of this scheme that not independently designed by the sender or receiver in the communication systems. Operation could lead in increase the security of encryption method so as to the system. On the other hand, the traditional encryption method and DNA Digital Coding are used to preprocess operation they can get completely different cipher text from the same plaintext of the message, which can effectively prevent attack from possible word as PCR primers. The complexity of biological difficult problem and cryptography computing difficulties provide a double layer security.

IV. PROBLEM STATEMENT

Email security is the most prominent are of work or the recent researchers. An email is something which is used by millions of the user per day for making their formal and informal communications. Among them the user might have their personal or professional data stored at their servers locations. Now is someone with malicious intensions gets control over the data, or the network then the confidentiality of the data and users privacy will be completely vanishes. Serving the users and organizations requirements on the security primitive is very cumbersome task. Now if the user demands something more customizable for its organization then it is not possible. Also the traditional security mechanism will work on same functionalities and mechanism which was open to explore for the attacker during the last few decades. During that time the system gets changes with technologies and security mechanism will remains as it was. Higher security demands will also serve financially more on the pockets of user and organizations. Thus there must be some approaches or framework which will reduces the cost burdensome and will increases the protection level with same type of mechanism. Apart from the above objective there are some problems identified open the previous security mechanism working for mail security. These are:

(i) Traditional approaches are totally based on the alphanumeric password which was easy to crack. Also the alphanumeric approaches are easily tracked out using key logger. There must be some approach which is case work as easy to remember but having more robust combinations for brute force attackers and key loggers will not work for that. Implicit password or image authentication will serve the objective here.

(ii) With previous system the user is not having any control over the security and if had somewhere with higher cost the configuration is a very tedious task. Thus with this work the security can be made user friendly for the operator.

(iii) If packet is captured by the fabricator or impersonator during the transmission, then the decryption can be performed if the encryption or cipher text or a portion of plaintext is known. But once the compression is performed then it is quite infeasible to decode the original message.

Some more modifications can be made here with the use of HTTPs, PGP and other security control over here.

The requirements of such mechanism are:

1) **Confidentiality of data:** No one can uncover information about data content from the query and response as well as the cipher texts itself after the above framework implementation.
2) **Privacy of the data owner**: No one can learn the actual identity of the data owner from the encrypted content.
3) **Integrity and Authenticity of Data**: It provides the correctness of the data which is sent by the user and the originality which is assured by the digital signature to confirm the source identity and its data ownerships.

V. PROPOSED APPROACH

This work suggests a novel email security framework using some of the well known security primitive. The concept mainly focuses on the secure access and authentication with data confidentiality up to the desired levels. It increases the protection level using the low risk based mailing system. The system is having various novel attributes and functionalities which were not implemented yet for email security and privacy. At the initial levels our approach seems to be at a higher level that the existing ones. It is well known that intermediate mediums that route emails between sender and recipients can be a real threat to privacy as these intermediate can be easily intercepted and tampered with email messages many software based solutions has been proposed to solve these problems such as P.G.P and P.E.M were developed, but these solutions were not good enough to provide security and various attacks can aimed to it and they can exploit the vulnerabilities of these management.

The system starts with a unique authentication system i.e. an image pattern authentication. Initially when the user gets itself registered for the system then the credentials of users are converted to the hash codes known as digest. Now this digest gets stored in the databases of the system. Next time when the user demands the access or control for the system this digest is verified and result of which gives the

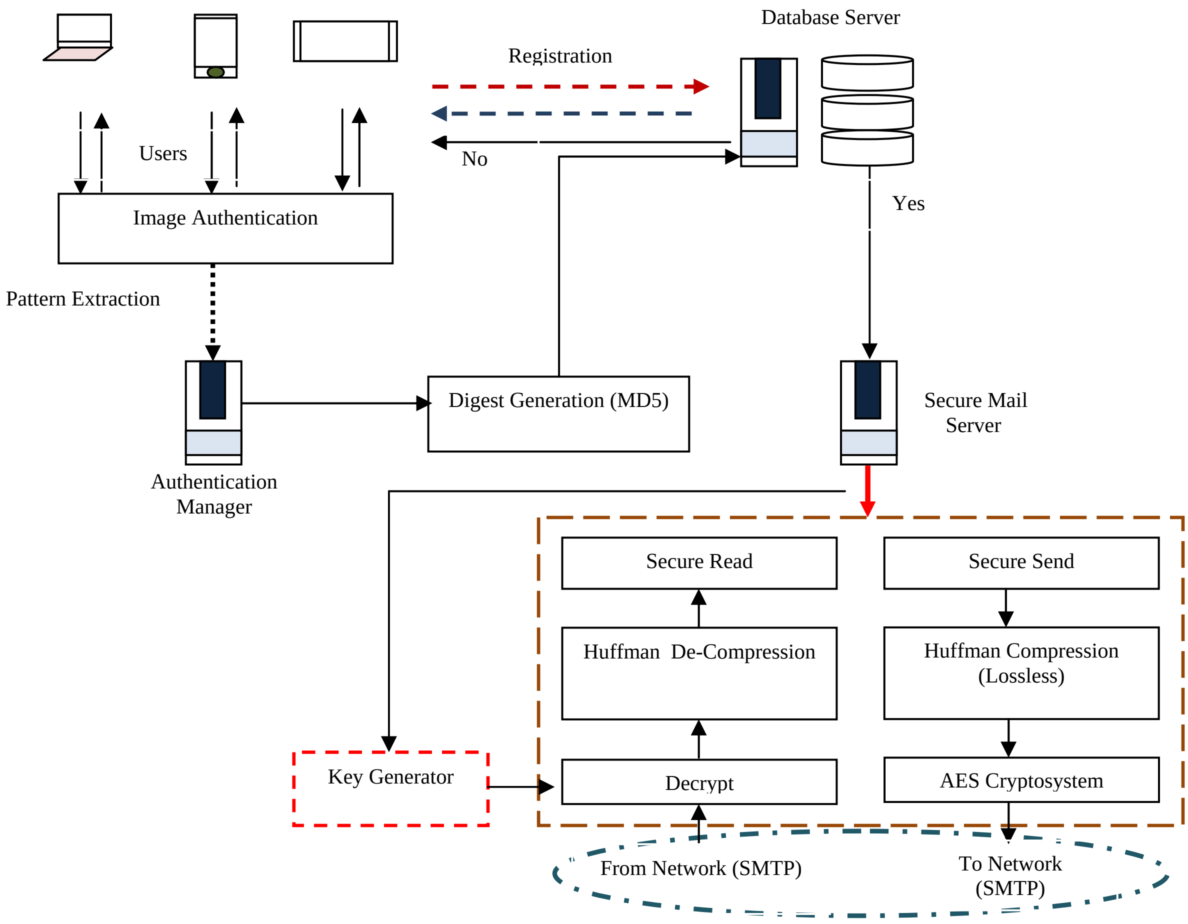

FIGURE 1: HYBRID EMAIL SECURITY FRAMEWORK FOR SECURE MAILS

complete control over the system. Now for image based authentication the image patterns using implicit authentication is selected. This pattern will act as the user's private information and is not accessible to anyone else.

Now this pattern is converted to hash values and stored in the database. Now next time if the same pattern for the image access at the login panel is repeated then only the digest will be matched and the control can be shifted successfully. For generating the digest well known algorithm of MD5 is used. This algorithm is having higher protection level with near optimal complexity which can sustain the value of the information.

Once the authentication is successful then the later operation of the security construct can be performed. Also it should be kept in mind that for serving the security over the network the protocol standard will also differ from the normal versions. Likewise for the HTTP the work uses HTTPs everywhere in web exchanges. Now once the digest mapping is performed the work will generate the key for the system which can be later on used for secure retrieval and sending. Now the phases are parted into two major zones. One will work for secure reading and another will work for secure sending.

For secure sending the first phase is compression. Here the compression used is lossless because the data on which the user works will not be loosed by the system. For tat the compression technique here used is Huffman Coding. It is simple and robust way of reducing the size of data without changing its original content. Once the compression is perfume the data can be encrypted using the AES encryption standard. Here the key passed is based on the previously generated digest based on the user image sequence patterns. For secure reading the process is reversed. Here the data is first decrypted using the same key generated by the digest. Later on the decompression is performed. Here the use is also given a control over the encoding phenomenon. Here this factor will serve the protection level to high satisfaction for the user. Here the encoding is served in two options 32 or 64. Now once all the security control is made available for user to configure then the trust over the system gets increased. The entire configuration is customizable for the user which raises the level of the system protection and is user friendly as well

VI. EXPECTED OUTCOMES

This mainly helps to protect an email against the various attacks.

- Secure emails transaction with encryption.
- Compression of data will minimized the overload of traffic over the communication channel

- The level of email security will increase.
- To retain reliability on third party location
- Client ensures about data storage in safe manner and unauthorized access.
- To protect data from different attacks at client end
- Might be became innovative approach at client end in cloud platform for different application domains.

VII. Conclusion

The email security can be done through various ways but the email encryption after compression is better approach in order to protect against the various attack. And this approach can be useful in lots of e-commerce application this can be useful mostly in the areas where the e-mailing is done such as, Banking system – various mails are sent to customer. Every Email service provider is taking advantage of cloud to dynamically enhance their capabilities. As we have seen that traditional approaches of authentication to the systems are not meeting the security requirements so a new system must be taken into the account. Our approach is taking advantages of best practices done under encryption and compression that makes the propped system more powerful and reliable for the consumers.

Reference

[1] Vijay varadharajan, *senior member, IEEE*, and udaya tupakula, *member, IEEE* "Security as a service model for cloud environment", published in ieee transactions on network and service management,vol. 11, no. 1, march 2014

[2] Zahir Tari, RMIT University "Security and Privacy in Cloud Computing" published By the IEEE computer society 2014

[3] Md. Asraful Haque, Babbar Imam, Nesar Ahmad " 2-ROUND HYBRID PASSWORD SCHEME" International Journal of Computer Engineering and Technology (IJCET), ISSN 0976 – 6367(Print),ISSN 0976 – 6375(Online) Volume 3, Issue 2, July-September (2012)

[4] Sadiq Almuairfi,Parakash Veeraraghavan and Naveen Chilamkurti" IPAS: Implicit Password Authentication System" Workshops of International Conference on Advanced Information Networking and Applications 2011.

[5] Mihir Bellare, Sriram Keelveedhi,Thomas Ristenpart" Message-Locked Encryption and Secure Deduplication" A preliminary version of this paper appears in the proceedings of Eurocrypt 2013.

[6] Andrej Bratko" Spam Filtering Using Statistical Data Compression Models" Journal of Machine Learning Research 7 (2006).

[7] Alexandra Boldyreva, Nathan Chenette, Adam O'Neill " Order-Preserving Encryption Revisited:Improved Security Analysis and Alternative Solutions" A preliminary version of this paper appears in Advances in Cryptology - CRYPTO 2011, 31st Annual International Cryptology Conference, P. Rogaway ed., LNCS, Springer, 2011.

[8] K. John Singh and R. Manimegalai “A Survey on Joint Compression and Encryption Techniques for Video Data" Journal of Computer Science 8 (5): 731-736, 2012.

[9] D. Prabhu ,M.Adimoolam ,P.Saravanna A Novel DNA based Encrypted Text Compression " IJCA Special Issue on “Network Security and Cryptography” NSC, 2011.

[10] V.Gopalakrishnan T.Purusothaman S.Annadurai S. Nitin Balaji" Enhancing Security through Compression, Randomized Encryption and Authentication" ICGST-CNIR Journal, Volume (5), Issue (3), October, 2006. [11] Ruisong Ye and Wei Zhou"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice" I. J. Computer Network and Information Security, 2012.

[12] Kristin Lauter “Can Homomorphic Encryption be Practical?" ACM 2012.

[13] Ms.B.Veera Jyothi, Dr.S.M.Verma, Dr.C.Uma Shanker “Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification" International Journal of Computer Applications (0975 – 8887) Volume 5– No.5, August 2010.

[14] Mojtaba Ayoubi Mobarhan, Mostafa Ayoubi Mobarhan and Asadollah Shahbahrami “Evaluation of Security Attacks on Umts Authentication Mechanism" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012