A Survey of Email Service; Attacks, Security Methods and Protocols

Haider M. Al-Mashhadi
University of Basrah,
College of Computer
Science and Information Technology,
Basrah, Iraq.

Mohammed H. Alabiech
University of Basrah,
College of Science, Basrah,Iraq.

ABSTRACT
Email security becomes a sensitive case to study in the field of information security. From the most important security issues of network is how to secure Email from the threats that can be exposed of the security of massages by attackers. In addition, what are the techniques that can be using to secure the Email? Different solutions and several standards levels have been fashioned according to the last security requirements that enhance the Email security. Some of the current enhancements concentrate on keeping the exchange of data through Email in an integral and confident way. While the others concentrate on authenticating the sender and confirm that, client will not repudiate from his message. This paper will explain Email works and discuss different threats in Email Communication and several Email security solutions. This paper introduces several models and techniques utilized to fix and enhance the safety of Email systems.

General Terms
Email, Security, Algorithms, Protocol

Keywords
Email security, Threats, Encryption, Filtering

1. INTRODUCTION
The Email security is the essential tool for business and communication, which are used more day after day. The Email is used for sending text, documents and data of tables at work and at home. Because of being the data transmitting is quite delicate process, the guarantee of these data is questionable and this represented a problem because the contract details of the competitive companies are unlimited, and the worse, there are capabilities for fraud Emails. On the other hand, the majority of Email files, although, are secured via reusable passwords, which are frequently weak and can be effortlessly haggled. One of the ways to save the watchword attack is to refrain from using passwords and to affirm a client without include secret key [1].

2. HOW DOES EMAIL WORK?
Email is sent as plaintext over networks all over the world utilizing the Simple Mail Transfer Protocol (SMTP)[2]. Email has been expanded to append error reporting/messaging and extra authentication to meet the increasing request of advanced Email. Mail Transfer Agents (MTAs) runs in the background, transporting message from host to host permitting message to be mailing across the world. You may have arrived via like MTA software program like Postfix, Qmail, Fetch mail, Sendmail.

The protocol SMTP permits per computer, which the message passes via to send on it within correct way to the end address. If one shut light on so much number of Email host over the worldwide, one can surprised how uncomplicated it everything appears

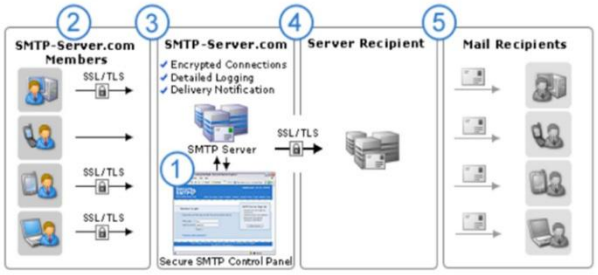

Fig 1: How does Email work[2].

Figure (1) shows a simple case of how Email are typically works, by sending the Email message from sender using SMTP, to the recipient.

1. Alice@yahoo.com sends out an Email to Bob@gmail.com.
2. Alice's Email receives by MTA at yahoo.com and queues (The waiting lists) it for delivery after all messages which are as well ready and requiring to go out.
3. On port 24, MTA yahoo.com meets MTA gmail.com. After yahoo.com admits the connection, the mail message sends out by the MTA at gmail.com. Then yahoo.com accepts and admits received of the message, closed connection.
4. The message put into Bob's incoming mailbox by The MTA gmail.com and in the next logs on, Bob will announce having new message.

Naturally, through this process different things can go faulty. It is important to mention some examples:

What happen when Bob does not be at gmail.com? In this situation, MTA at gmail.com refuses the message and advise MTA at yahoo.com about the fault. The MTA at yahoo.com will produce and send a message to Alice@yahoo.com, making known her that no Bob at gmail.com.

What goes on if gmail.com does not respond to yahoo.com's connection attempts?

(May be the server (host) is off for maintenance or repair). MTA at yahoo.com apprises Alice that the first delivery try has went wrong.

The server manager will determine more tries at time interval until reach to the deadline; Alice will be informing that message is undeliverable.

Nowadays as for the security related subjects, protocols invents for the safe transfer of Email messages [2].

3. THREATS IN EMAIL COMMUNICATION

3.1 Eavesdropping

Email letters move over nets that are fractions of a great image i.e. Internet with a great deal of people on it. Hence it's quite simple for some person to capture or track letter and read it[3,4] and to overcome the Eavesdropping, encryption services can be employed[5].

3.2 Identity Theft

If not right security protocols are adopted that attacker may capture or steal your username and password and utilized to read your messages, it may be possible. Moreover sending Email letters from your account while you do not have any idea [3] and to overcome the Identity Theft, enhance the user skills can be used.

3.3 Message Modification

Any person whom gets your messages, can change it too if they are unencrypted. Moreover any person has administrative rights to visit your message on whatever of SMTP host can not only see your message but can as well change it [3] and to overcome the Message Modification, Strong Hop Integrity Protocol can be utilized[6].

3.4 False Messages

The name of the sender can be fabricated easily, then it is very simple to send message which seems that has been sent by someone else unprotected[3] and to overcome the False Messages, develop the user skills can be utilized in order to ability to distinguish false message.

3.5 Unprotected Backups

Messages generally can be reserved in plaintext on SMTP server and backups can be creating. The messages can be residing on the severs(backup servers) for several yrs even if you have deleted the message. So any person who accesses those servers can read or access also your letters [3] and to overcome Unprotected Backups, the clients should deal with highly credible server.

3.6 Repudiation

It is recognized that Email messages can just be faked; therefore any person who sends you some messages on reject concerning can later on reject concerning can later sending a message and to prove it is not easy. The implications of this forging problems are the same of contracts in business communications [3] and to overcome Repudiation the sender must use the digital signature [5].

3.7 Email spoofing

Sometime Email seems to be obtained from an authentic source but actually it has been sent from somewhere else[3,7,8] and to overcome Email spoofing, Transport Layer Security and its predecessor, Secure Sockets Layer (TLS /SSL) can be applied to enforce authentication[3].

3.8 Email Spamming

Junk or spam refers to the posting of Email to number of individuals for several malicious aim or whatever use of advertisement. Spam rosters sending are created always by stealing mailing list or by searching info from internet[3,9] and to overcome Email Spamming, Email filtering can be used depending on the Email content[10].

3.9 Email Bombing

Email “bombing” indicates to very mail sending over and over by an offender to a specific user[3,4] and to overcome Email Bombing, filtering Queued Email can be utilized dependent on the developed rule sets[11].

3.10 Sending threats

Menacing mails are transferring to persons who or to inflame them, or to disturb their state of temper, to take some unfavorable stage. Occasionally fake data are also sent on to 3rd users or parties to injure the reputation of specific individual. It is known as aspersion, a communication is not regard defamatory unless it is sent on to some person differently the target[3] today several of the common characteristics in mail security products contain filtering services such as antispam, antivirus, HTML tag removal, confidentiality checks, inappropriate content scanning[12].

3.11 Email Frauds

Email Fraud is the universal adulteration made for some personal benefits or monetary gain[3] and to overcome the Email Frauds, increase the user skills can be applied in order to ability to distinguish Email Frauds and by using Email filter [10].

3.12 Emails used as devices to spread malicious software

The attacker can be using Emails as devices to distribute worms, viruses, and other malicious software. These Emails are attached to ours as attachment, when you open them they will attack your browser or computer[3], filtering services can be used such as antivirus, antispam to overcome it[12].

3.13 Phishing

It can be known as an attack to larceny your secret info. It can be defined as an attack to steal your confidential information for example bank credentials, passwords and ATM PIN. It conforms as Emails which comes to your count and which seems to be from some authenticated side, such as your depository financial institution. These Emails attract you to open hyperlink exists at your Email or reply to message or click on attach file and that click will direct you to their website but it seems actually as your trusted site of depository financial institution and ask you to fill several secret info like passwords, hence stealing your password and using it later for any malicious intent[3,13,14]. Specified spam filters can decrease the phishing Emails number that achieve their addressees' inboxes, or supply post-delivery remediation, removing and analyzing phishing attacks. These approaches depend on machine learning [15].

4. EMAIL SECURITY TECHNIQUES

The Email security technique should include an important set of cryptographic mission. It supplies the below cryptographic missions[16].

- Encryption: The procedures that converts plain message into cipher message.
- Non-repudiation: Recipient can prove that the sender really sent it. Non-Repudiation (Origin): Confirm an Email was transferred by specific aspect, Non-repudiation (Destination): Confirm an Email was obtained by specific aspect.
- Integrity: defending against destruction or wrong information change, the sent Email is does not alter. The guarantee that message received is competently as transferred by a licensed entity.

- Privacy: "preserving authorized restrictions on information access and disclosure" [5].
- Authentication: is a property that an Email has not been altered, when in transit.
- Proof of submission: Confirmation to the sender that the mailer got it.
- Proof of delivery: Confirmation to sender that the recipient got it.

Now, this study survey below the important methods that used in Email security:

4.1 Multilevel Security

4.1.1 Email Security Using Encryption and Compression

This work uses a Codebook to Sending Email as a conventional way to supply privacy. Algorithms of Compression, Decompression, Encryption and Decryption will add the protection to sending messages over internet. In spite of the key is defined also from the id of the receiver's user and the character is changed to ciphertext with various key and key has increased by one at any moment. The algorithm suggests the next features, firstly, Encryption messages to secure Email, secondly, reducing the traffic overload in transmission channel by the message compression [17].

4.1.2 A Uniform Approach for Multilevel Email Security Using Image Authentication, Compression, OTP & Cryptography

To secure Email files, this technique suggests novel multilevel Email security structure design. The proposed structural design deals with three standard of security that is picture confirmation through model matching, pressure & cryptography in light of characteristic. The course messages in the middle of sender and recipient can be a real danger to security as these halfway can be effortlessly capture and become corrupted with Email messages many programming founded arrangements has been suggested to solve these matter. This way proposes a secure confirmation management construction styling Image Sequence Authentication-Compression & Cryptography (ISA-CC) that is picture based on and wipes the requirement for including passwords [1].

4.2 Encryption

4.2.1 Design of Fully Deniable Authentication Service for Email Applications

Email authentication service will be a full deniable in this method, it can be easy incorporated the work purpose into the existing Secure/ Multipurpose Internet Mail Extensions(S/MIME) and Pretty Good Privacy(PGP) to supply message authentication without nonrepudiation evidence. The goal of this method can be just a particularized message receiver to message authentication. This technique as well permits the sender of message be able to refuse message generation. The advantage from this way can save the privacy of personal message [18]

4.2.2 New Secure E-mail Scheme Based on Elliptic Curve Cryptography Combined Public Key

This method to supplies rather perfect security like data integrity, authentication, data confidentiality and nonrepudiation of origin. It not necessity to preparation the third online certificate agent when Compare with another protocols to secure the Email like S/MIME or PGP, necessitates little space to storage the key, takes smaller the capability from computing, in addition to be often easier than another systems for the Email security. The proposed method is particularly desirable for the implementation in intranet environment and private network [19].

4.2.3 A Secure Email System Based on IBE, DNS and Proxy Service

The study suggests a new system for Email security, depends on Identity Based Encryption (IBE) that utilizes DNS as the base for a proxy service, key exchange, which implements encryption operation and decryption instead of user and a fingerprint authentication system or secure key token for authentication the user. In the work approach, each current functionality of Email is kept, and no Modern infrastructure is desired. This strategy able to decrease phishing significantly and probably extenuate spam [16].

4.2.4 Secure Server Verification by Using RSA Algorithm and Visual Cryptography

This work utilizing RSA Algorithm and Visual Cryptography (VC) to resolve the phishing problems. There is an image here depend authentication-utilizing VC. Unique keys have been kept by trusted server for request of users for images encryption and decryption. The method chooses stochastic image for registration process. Then implement cryptography and Image Converter into two parts. First part be send after encryption to trusted server for tests. Supplied encrypted version of part just when server under test is registered with trusted server. Sending part back to user. Receive the part and to gain an image must implement decryption. If there is a match between the original image and this image, the web site can be applying for more transaction [20].

4.2.5 Secure Mail Using Visual Cryptography

The method applying visual cryptography on Email to be send by transforming into a gray scale image. The gray scale image is produce (2 , 2) visual cryptographic shares. Encrypt the shares applying a chaos-based image encryption algorithm applying wavelet transform and authenticated utilizing public key depend authentication technique. The first share sent to a server while the other to mail box of the recipient. The potentiality for attack from man in the middle is impossible because the operation of transmission of the two-shared parts is transmitting via two Different medium of transport. If an attacker has from two shares just one part, so no information can the attacker obtain concerning the message at the recipient side, he can recovery the grey scale image through of fetch the two shares, decrypted and stacked. Finally, the message is restoring from the grey scale image [21].

4.2.6 Secure Server Verification

This way proposed a new approach by applying RSA algorithm and Visual Cryptography. Cryptography is the ordinarily utilized method to data protection. In this work, image is not created, instead it is supplied by the server or user able to browse the image. Attackers would not be capable to crack the encrypted image by any technical way. The main aim of the method is to protection users from identify theft of the users of the system and from fraudulence [22].

4.3 Filtering

4.3.1 Ripper Algorithm

This method proposes new ways for automatically learning bases for sorting Email into several classes; even so it didn't specially address the class of junk Email in this method [23,24].

4.3.2 Genetic Document Classifier

The work uses genetic programming technique to improve classifying agents. This is a novel method for classifying documents, where all agents develop representation of a parse-tree of a user's specific information necessity. The other remarkable properties of work are a continual training process; user's feedback assists the agent to adapt long-term information requirements for the user [23,25].

4.3.3 Smokey

This method identifies several approaches to flame recognition admitting a prototype system. This is supporter for an Email that able to find hostile Emails. Smokey erects a 47-component feature vector depended on the semantics and syntax of all clause, integrating the sentences vectors in all message. A training set of 720 messages was utilized by Quinlan's C4.5 decision-tree generator to define characteristic-depended rules which were can to right categorize 98% of the nonflames and 64% of the flames in a detached experiment set of 460 messages [23,26].

4.3.4 Bayesian Junk Email Filter

A junk Email filter depends on a promoted Naïve Bayes classifier. Recall and accuracy were amended when header particular information and phrases were appended as characteristics [23,27].

4.3.5 An Email Classification Scheme Based on Decision-Theoretic Rough Set Theory and Analysis of Email Security

New system is introduced to class Emails to 3 sets spam, nonspam and suspicious, it depended on decision-theoretic rough sets. When comparing with common categorization ways such "Naïve Bayes classification", the filter of anti-Spam model decrease the errors rate that distinguish a non-spam from spam, and it can detect prospective safety problems of several Email systems. A way based on the Email classification paradigm was developed, a way based on Email classification paradigm was sophisticated, and can distinguish the new messages to three class – firstly spam, secondly nonspam and thirdly suspicious instead of no more categorization the forthcoming messages as spam and non-spam [23].

4.3.6 Research on Email Filtering Based on Improved Bayesian

This method merged Bayesian algorithm with Boosting method, offered a new filter spam algorithm. Bayesian algorithm neglects the import info. The experience indicates that the algorithm able to resolve it. The method's results displays that the amended algorithm has more beneficial and best accomplishment. The enhanced filtering algorithm cannot only enhance the precision of spam filter, but as well decrease the information loss and the error ratio of misclassifying Email [28].

4.3.7 A Novel Method of Spam Mail Detection Using Text Based Clustering Approach

The method suggests clustering for Email and performed to effective find the spam messages. The suggested work includes the distance between all of the email properties. Clustering is the way which applied for data stenography. It separates the data to sets based on resemblances of pattern like that every set is summarized through single or more representative, there is an increasing confirmation on exploratory test of so big datasets to detect helpful types, it's named data mining. The supposing work in this method, an effective clustering algorithm combining the characteristics of BIRCH algorithm and K-means algorithm which showed. K-Nearest-neighbor distances and Nearest-neighbor distances able to do as the foundation of categorization of test data on the basis of learning under the supervision of. Classifier prophetic precision is computed for the clustering algorithm. In addition to various appraisal measures are applied to analyze the execution of the clustering algorithm sophisticated in group with the different classifiers[29].

4.3.8 Efficient Spam Filtering System Based on Smart Cooperative Subjective and Objective Methods

This method suggests an active method for spam filtering which is depending on an intelligent subjective cooperative way for filtering the content in add-on to the quickest and the most credible without content-based topical ways. A new method for filter of spam which integrates both a traditional spam filtering methods and the smart cooperative subjective spam filtering method is presented. The system integrates various applications. The firstly is a web rely strategy which we have sophisticated which depended on the suggested method. A server implementation has additional characteristics appropriate for the companies and closed work sets is another portion of the scheme. Other portion is a collection of regular web serving that permit each Email client or server to react with the system. The work permits the Email servers to implementing the system for the Email filtering. They able to permit the clients by the mail user agents to take part in the issue of filter of spam[30].

4.3.9 An Innovative Approach for Detecting Targeted Malicious E-mail

This way explicates how the malicious Emails are categorizing and how these are remove and know the contents of messages. In order to classify here the method is utilizing an Email filtering, Bayesian spam filtering and J48 process that overcomes the troubles happened in linear C-Support Vector Machine (C-SVM). This machine affords the precise results when contrasted to the existing one. There are three steps to check firstly is to find the malicious Email secondly is use classifier to classify awarding to the Emails received and send out to trash automatically and omit directly[31].

4.3.10 Email Spam Filtering Using Adaptive Genetic Algorithm

This technique introduced a genetic algorithm based way for filter Email from spam was debate with its disadvantages and advantages. The outcomes offered in this work are grater and proposed that genetic algorithm can be a well choice in coupling with other techniques for Email filter can supplying more strong resolution. This algorithm successfully recognizes spam Email. The performance of the process relies on the genetic algorithm parameters and dataset. The suitability of the algorithm is more than 82% [9].

4.3.11 Detection of Fraudulent Emails by Employing Advanced Feature Abundance

This method presents a model of fraudulent Email detection utilizing advanced feature choice. The method extracted several types of features and compared the execution of each class of features with the others in terms of the fraudulent Email discovering rate. The way used different classification algorithms including NB, SVM, CCM and J48. The different types of features are integrated step by step. The experimentations have been executed on different diverse feature sets and the diverse classification ways. The comparability of the results is as well presented and the rating show that for the fraudulent Email detecting tasks, the feature set is more significant anyway of classification method. The results of the work propose that the task of fraudulent Emails detecting needs the best choice of feature set; while the choice of classification way is of less importance. The work accomplished the precision of fraudulent Email detection about 96%. [32].

4.3.12 Online Imbalanced Support Vector Machine for Phishing Emails Filtering

Standard Support Vector Machine (SVM) could give sub optimal results on filtering phishing Emails, and it oftentimes requires a lot time to implement the classification for big data sets. In this way, an online version of imbalanced SVM (OISVM) is suggested. Firstly an Email is converted into twenty features which are well selected depend on its content and link characters. Secondly, OISVM is evolved to optimize the classification truth and decrease computation period, which is used a novel technique to regulate the separation hyperplane of imbalanced date groups and an online algorithm to make the retaining process very fast. As compared to the present methods, the tentative results present that OISVM can realize significantly utilizing a proposed expressive evaluation way. The experiments results show that OISVM can obtain so good results with the various validation datasets employed. Furthermore, a number of features have described that are particularly well suited to filtering phishing mails [33].

4.3.13 An Online Malicious Spam Email Detection System Using Resource Allocating Network with Locality Sensitive Hashing

This method suggests a new on-line system, that is able to find quickly spams and to adjust the alters in the Emails and the Uniform Resource Locator (URL) links directing into the web sites of malicious through the system update every day by means of insert an independent task about a server to yield training models, in that dual recoil Emails are automatically gathered and their category labels have been afforded by a "crawler-type software" to anatomize the web site maliciousness named "SPIKE". In universal, since senders apply persuasion to diffusion many malicious messages for Email within a few interval, this spread spam oftentimes have the comparable contents or match. Thus, it is not needful for whole spam Email to be learned. New kids of spam should be chosen for learning and this is able to be accomplished in order to adjust to incoming malicious attacks rapidly and this is able to be accomplished through inserting an effective learning method to a classifier pattern. Through such aim, method assumes Resource Allocating Network with Locality Sensitive Hashing (RAN-LSH) as a classifier type with a data selection function. In RAN-LSH, the similar or corresponding spam which have previously been learned are speedily inspected for a hash schedule in Locally Sensitive Hashing (LSH), where the identical comparable Emails existed in "well- learned" are ignored without being utilized as training data. To analyze Email messages, method adopts the Bag of Words (BoW) produces and procedure feature vectors. The features of it depend on the Term Frequency- Inverse Document Frequency (TF-IDF) which has been normalized[34].

4.4 Security Protocols

4.4.1 Secure E-mail Protocols Providing Perfect Forward Secrecy

There are two protocols for Email in this way suggested. The two protocols for secrecy rely on the Certificate of Encrypted Message Being a Signature (CEMBS) and Diffie-Hellman key are proposed. The CEMBS is applied to convince a verifier that a ciphertext is actually a certain party's signature on a public info whilst without signature exposing. The two protocols are appropriate for Email system in the genuine world and can supply idealistic forward secrecy. The first one, the recipient claims a portable system, i.e. smart card to recall a utilized secret random integer for each round and keep it for short term key computation, this key is construct under Diffie-Hellman key exchange. Except sender and receiver no one can compute the short term key shared between the two parts (sender and recipient). So, if sender's secret key is exposed, it will no way detect the short term key. Hence, all past Emails can be remain secure. The second protocol is similar to first protocol and more pliable and appropriate to the Email system and used Diffie-Hellman to construct the short term key. This protocol applying CEMBS to prevent the mail server from knowing the short-term key. If sender's password or secret key is exposed, an attacker can only obtain the secret exponent or signature. Therefore, the attacker will not obtain the short term key only if both sender's password and secret key are exposed at the same time. Even both compromised at the same time; only at this time the attacker can gain the short term key. Former short term keys cannot be detect because the short term key is construct under the Diffie-Hellman key exchange. Hence, this protocol renders perfect forward secrecy (PFS) [35].

4.4.2 Robust Email Protocols with Perfect Forward Secrecy

The method proposes two feasible Email protocols supplying PFS in which an extra short term key is determined between a recipient and an Email server applying the Diffie-Hellman key exchange. The first protocol has the feature that a signature algorithm encryption or an encryption can be performed applying any public key algorithm. The second protocol realizes competence and ideal forward secrecy at the same time [36].

4.4.3 SMEmail - a New Protocol for the Secure Email in Mobile Environments

A new secure protocol of application layer, named SMEmail, is presented which supplies diverse security properties like authentication, integrity, non-repudiation, confidentiality, and send on message confidentiality secrecy for the Emails. SMEmail presents an elliptical curve-based public key resolution that utilizes public keys for the saved keys establishing of a symmetrical encryption, and is so desirable for the resource-limited program such as mobile phones [37].

4.5 Finger Print Authentication Scheme

4.5.1 A Secure Email System Based on Fingerprint Authentication Scheme

This method suggests a new secure Email system depends on a fingerprint authentication scheme that integrates IBE scheme with fingerprint authentication technology. The system completely solves the present problems faced in Email safety protection implementations [38].

4.5.2 Using Fingerprint Authentication to Reduce System Security - An Empirical Study

In this study, (96) volunteers each created a two accounts, one secured just by a password and other secured by both a password plus a fingerprint reader. Consequences of study assist robustly the hypothesis-on average. As utilizing the reader of fingerprint, created passwords of users which could take one three-thousandth so long as to fracture, that way probably deleting the feature of two factor authentication could have presented [39].

4.6 Enhanced User Skills

4.6.1 Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System

This method depicts the evaluation and design of an embedded training Email system that learns users concerning phishing through plain Email use. Experiments contrasting the performance of standard security notices on phishing with two embedded training designs that had been conducted is sophisticated. Embedded training is more active than the present exercise of sending security observation. The results propose that the existing exercise of posting out security notifications is fruitless and refer that all embedded training interferences assist inform people about phishing and to avert phishing attacks. Sound design rules is derived for embedded training systems [40].

4.6.2 Security services as coping mechanisms: an investigation into user intention to adopt an Email authentication service

This method checks the ingredients that influence user intent to apply an Email authentication service. The outcomes indicate that user intent to arrange an Email security service is conditional upon users' understanding of estimate and danger of the strategies of external and internal coping. The work takes part in survey in information security behavior, design and service success design and security service adoption [41].

5. EVALUATION

Table (1) describes a comparison among all protocols mentioned in this paper, and the solutions that used in these methods and protocols to solve the problem of email security.

Based on this table, it is possible to conclude the following points:

- In Multilevel Security group, "A uniform approach for multilevel Email security using image authentication, compression, OTP & cryptography" technique is the best one because provides authentication, confidentiality and message compression.
- In Encryption group, "A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key" method is the best technique because provides authentication, confidentiality, Integrity and nonrepudiation and this technique applied elliptic curve cryptography which provides strong cipher text.
- In Filtering group, all techniques are specialized in detect the threats message based on classification.
- In Security Protocols group, all techniques are provide authentication, confidentiality, Integrity and nonrepudiation but "Robust Email Protocols with Perfect Forward Secrecy" method is enhanced for "Secure E-mail Protocols Providing Perfect Forward Secrecy" method and "SMEmail - A New Protocol for the Secure Email in Mobile Environments" method is use only for Mobile platform.
- In Finger Print Authentication Scheme group, surely the "A Secure Email System Based on Fingerprint Authentication Scheme" technique is the best because provides authentication, confidentiality, Integrity and nonrepudiation.
- In Enhanced User Skills group, the first method used for detects the phishing message and the second method use for Email authentication services.

6. CONCLUSION

Email security becomes a sensitive case to study in the field of information's security because Email communication is an increasing as a major way for organizations and individuals to communicate. However, unfortunately, this is also an emerging method of directing crime in the cyber world, e.g. virus attacks, identity theft etc. Many threats are confronted by client because of attenuating circumstances existent in the system, and then there is necessary to make Email system sturdier by defeating the existing security faults, hence Email security becomes very important case to study in the field of information security. This paper presents different threats in Email Communication and several Email security solutions. There are many security problems with Email and many of the solutions to every problem and there is no comprehensive solution for all Email security problems, but there are many combined methods to make the Email system more and more security. The future goal of this study is the idea of rendering the paper to all persons who are interested in the security of Email in order to have a clear concept about the idea of email and the most important threats that plague email and methods of treatment or prevention.

Table 1. Comparison among the Email security methods

Group	Technique	Authen.	Confid.	Integ.	Nonrepud.	Comp.	Filter.	PFS
Multilevel Security	Email Security using Encryption and Compression	---	for message	---	---	for message	---	---
	A uniform approach for multilevel Email security using image authentication, compression, OTP & cryptography	for user	for message	---	---	for message	---	---
Encryption	Design of Fully Deniable Authentication Service for E-mail Applications	for sender	for message	for message	for sender	---	---	---
	A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key	for sender	for message	for message	for sender	---	---	---
	A Secure Email System Based on IBE, DNS and Proxy Service	for login	for message	---	for sender	---	---	---
	Secure Server Verification By Using RSA Algorithm And Visual Cryptography	for login information	---	---	---	---	---	---
	Secure Mail using Visual Cryptography (SMVC)	for sender	for message	for message	---	---	---	---
	Secure Server Verification	for login information	---	---	---	---	---	---
Filtering	Ripper Algorithm	---	---	---	---	---	from hostile Email	---
	Genetic Document Classifier	---	---	---	---	---	from hostile Email	---
	Smokey	---	---	---	---	---	from hostile Email	---
	Bayesian Junk Email Filter	---	---	---	---	---	from junk Email	---
	An Email Classification Scheme Based on Decision-Theoretic Rough Set Theory and Analysis of Email Security	---	---	---	---	---	from spam Email	---
	Research on E-mail Filtering Based On Improved Bayesian	---	---	---	---	---	from spam Email	---
	A Novel Method of Spam Mail Detection Using Text Based Clustering Approach	---	---	---	---	---	from spam Email	---
	Efficient Spam Filtering System Based on Smart Cooperative Subjective and Objective Methods	---	---	---	---	---	from spam Email	---
	An Innovative Approach for Detecting Targeted Malicious E-mail	---	---	---	---	---	from spam Email	---
	Email Spam Filtering Using Adaptive Genetic Algorithm	---	---	---	---	---	from spam Email	---
	Detection of Fraudulent Emails by Employing Advanced Feature Abundance	---	---	---	---	---	from spam Email	---

Group	Technique	Authen.	Confid.	Integ.	Nonrepud.	Comp.	Filter.	PFS
Filtering	Online Imbalanced Support Vector Machine for Phishing Emails Filtering	---	---	---	---	---	for phishing Email	---
	An Online Malicious Spam Email Detection System Using Resource Allocating Network with Locality Sensitive Hashing	---	---	---	---	---	from spam Email	---
Security Protocols	Secure E-mail Protocols Providing Perfect Forward Secrecy	for sender	for message	for message	for sender	---	---	for short term key
	Robust Email Protocols with Perfect Forward Secrecy	for sender	for message	for message	for sender	---	---	for short term key
	SMEmail - A New Protocol for the Secure Email in Mobile Environments	for sender	for message	for message	for sender	---	---	for message
Finger Print Authenticati	A Secure Email System Based on Fingerprint Authentication Scheme	for login for sender	for message	for message	for sender	---	---	---
	Using Fingerprint Authentication to Reduce System Security - An Empirical Study	for login	---	---	---	---	---	---
Enhanced User Skills	Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System	---	---	---	---	---	for phishing	---
	Security services as coping mechanisms: an investigation into user intention to adopt an Email authentication service	Email authentic. services	---	---	---	---	---	---

7. REFERENCES

[1] Apeksha Nemavarkar, Rajesh Kumar Chakrawarti, 2015. "A uniform approach for multilevel Email security using image authentication, compression, OTP & cryptography". In Proceedings of the IEEE International Conference on Computer, Communication and Control IC4.

[2] Sunny gill, Gaurav Rupnar, Vaibhav Ramteke, Dipti Patil and Vijay M.Wadhai, "Email Security Protocol", International Journal of Computer Trends and Technology- March to April Issue 2011.

[3] Gurpal Singh Chhabra, Dilpreet Singh Bajwa, "Review of Email System, Security Protocols and Email Forensics", International Journal of Computer Science & Communication Networks, Vol. 5(3), 201-211, January 2015.

[4] Olalekan Adeyinka, May 2008. "Internet Attack Methods and Internet Security Technology". In Proceedings of the Second Asia International Conference on Modeling & Simulation.

[5] William Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, 2011.

[6] M. G. Gouda, E. N. Elnozahy, C.-T. Huang and T. M. McGuire, "Hop Integrity in Computer Networks", IEEE/ACM Transactions on Networking, Vol. 10, Issue: 3, Jun 2002.

[7] Kunal Pandove, Amandeep Jindal and Rajinder Kumar. "E-Mail Spoofing", International Journal of Computer Applications, Vol. 5, No.-1, pp- 27-30, August 2010.

[8] P. Ramesh Babu, D. Lalitha Bhaskari and CH. Satyanarayana, "A Comprehensive Analysis of Spoofing", International Journal of Advanced Computer Science and Applications, Vol. 1, No.-6, Dec. 2010.

[9] Jitendra Nath Shrivastava, Maringanti Hima Bindu, "Email Spam Filtering Using Adaptive Genetic Algorithm", I.J. Intelligent Systems and Applications, 54-60, 02, January 2014.

[10] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker and Stefan Savage, May 2011. "Click Trajectories: End-to-End Analysis of the Spam Value Chain", Oakland, CA: In Proceedings of the IEEE Conference on Security and Privacy (SP).

[11] Tim Bass, Alfredo Freyre, "E-Mail Bombs and Countermeasures: CyberAttacks on Availability and Brand Integrity", IEEE Network , Vol. 12, Issue:2 , Mar/April 1998.

[12] Pam Cocca, "Email Security Threats", GIAC Security Essentials Certification (GSEC) Practical Assignment - Version 1.4b Option1, September 20, 2004.

[13] Kim-Kwang Raymond Choo, "The Cyber Threat Landscape: Challenges and future Directions", Journal of

Computer and Security, Science Direct, Elsevier, Vol. 30, Issue 8, pp-719-731, 2011.

[14] Gori Mohamed .J, M. Mohammed Mohideen and Shahira Banu. N, "E-Mail Phishing-An Open Threat to Everyone", International Journal of Scientific and Research Publications, Vol. 4, No.-2, Feb. 2014.

[15] Cleber K., Olivo , Altair O., Santin , Luiz S. and Oliveira, "Obtaining the Threat Model for E-mail Phishing", Journal of Applied Soft Computing, Science Direct, Elsevier, Vol. 13, Issue 12, Pages 4841–4848, Dec. 2013.

[16] Suresh Kumar B., Jagathy Raj V. P., "A Secure Email System Based on IBE, DNS and Proxy Service", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 9, Sep. 2012.

[17] Yogendra Kumar Jain, Pramod B. Gosavi, 2008. "Email Security using Encryption and Compression", In Proceedings of the IEEE International Conference on Computational Intelligence for Modelling Control & Automation (CIMCA).

[18] Lein Harn, Jian Ren, "Design of Fully Deniable Authentication Service for E-mail Applications", IEEE Communications Letters, Vol. 12, No. 3, March 2008.

[19] Yi Zhang, Tianxi Cui and Hong Tang, 2008. "A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key". In Proceedings of the IEEE International Conference on Network and Parallel Computing (NPC).

[20] Aboli Bhanji, Priyanka Jadhav, Sayali Bhujbal and Punam Mulak, "Secure Server Verification By Using RSA Algorithm And Visual Cryptography", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 4, April 2013.

[21] Ajish S, Rajasree R., 2014. "Secure Mail using Visual Cryptography (SMVC)". In Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT), Hefei, China.

[22] Shweta Umredkar, Snehal Badhe and Hemali kondhekar, "Secure Server Verification", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 4 Issue 4, April 2015.

[23] Wenqing Zhao, Yongli Zhu, 2005. "An Email Classification Scheme Based on Decision-Theoretic Rough Set Theory and Analysis of Email Security", In Proceedings of the TENCON IEEE Region 10 Conference.

[24] Cohen, W., 1996. "Ripper Algorithm", Learning Rules that Classify Email. In Proceedings of the AAAI Spring Symposium on Machine Learning in Information Access, Palo Alto, US: pp.18-25.

[25] Clack, C., Farrington, J., Lidwell, P., and Yu and T., 1997. "Genetic Document Classifier", Autonomous Document Classification for Business. In Proceedings of The ACM Agents Conference, pp.201-208.

[26] Spertus, E., 1997. "Smokey:Automatic Recognition of Hostile Messages". In Proceedings of Innovative Applications of Artificial Intelligence (IAAI),AAAI Press, pp.1058-1065.

[27] Sahami, M., Dumais, S., Heckerman, D., and Horvitz and E., 1998. "A Bayesian Approach to Filtering Junk Email, in Learning for Text Categorization", Papers from the Workshop AAAI Technical Report WS-98-05.

[28] Liu Pei-yu, Zhang Li-wei and Zhu Zhen-fang, "Research on E-mail Filtering Based On Improved Bayesian", Journal of Computers, Vol. 4, No. 3, March 2009.

[29] M. Basavaraju, R. Prabhakar, "A Novel Method of Spam Mail Detection using Text Based Clustering Approach", International Journal of Computer Applications (0975 – 8887), Vol. 5– No.4, August 2010.

[30] Samir A. Elsagheer Mohamed, "Efficient Spam Filtering System Based on Smart Cooperative Subjective and Objective Methods", International Journal Communications, Network and System Sciences, Vol. 6, Issue 2, 88-99, Feb. 2013.

[31] B.V.R.R.Nagarjuna, V. Sujatha, "An Innovative Approach for Detecting Targeted Malicious E-mail", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 2, Issue 7, July 2013.

[32] Sarwat Nizamani, Nasrullah Memon, Mathies Glasdam and Dong Duong Nguyen, "Detection of fraudulent Emails by employing advanced feature abundance", Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University Egyptian Informatics Journal, Vol. 15, Issue 3, 169–174, 2014.

[33] XiaoQing Gu, TongGuang Ni and Wei Wang, "Online Imbalanced Support Vector Machine for Phishing Emails Filtering", TELKOMNIKA Indonesian Journal of Electrical Engineering Vol. 12, No.6, pp. 4306 - 4313, June 2014.

[34] Siti-Hajar-Aminah Ali, Seiichi Ozawa, Junji Nakazato, Tao Ban and Jumpei Shimamura, "An Online Malicious Spam Email Detection System Using Resource Allocating Network with Locality Sensitive Hashing", Journal of Intelligent Learning Systems and Applications, Vol. 7, Issue 2, 42-57, 2015.

[35] Hung-Min Sun, Bin-Tsan Hsieh, and Hsin-Jia Hwang, "Secure E-mail Protocols Providing Perfect Forward Secrecy", IEEE Communications Letters, Vol. 9, No. 1, January 2005.

[36] Bum Han Kim, Jae Hyung Koo and Dong Hoon Lee, "Robust Email Protocols with Perfect Forward Secrecy", IEEE Communications Letters, Vol. 10, No. 6, June 2006.

[37] Mohsen Toorani, Dec. 2008. "SMEmail - A New Protocol for the Secure Email in Mobile Environment", In Proceedings of the IEEE International Conference Reprinted from the Proceedings of the Australian Telecommunications Networks and Applications (ATNAC'08), pp.39-44, Adelaide, Australia.

[38] Zhe Wu, Jie Tian, Liang Li, Cai-ping Jiang and Xin Yang, 2007 "A Secure Email System Based on Fingerprint Authentication Scheme", In Proceedings of the IEEE International Conference on Intelligence and Security Informatics.

[39] Hugh Wimberly, Lorie M. Liebrock, 2011. "Using Fingerprint Authentication to Reduce System Security - An Empirical Study", In Proceedings of the IEEE

International on Symposium on Security and Privacy, IEEE.

[40] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong and Elizabeth Nunge, 2007. "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System", In Proceedings of The free and open access Conference organize by the School of Computer Science at Research Showcase, accepted by Human Computer Interaction Institute.

[41] Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur & H. Raghav Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an Email authentication service," Information Systems Journal, Vol. 24, Issue 1Pages 61–84 24, January 2014.