Journal of Information Security, 2015, 6, 1-11
Published Online January 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.61001

Scientific Research Publishing

Study of the Security Enhancements in Various E-Mail Systems

Afnan S. Babrahem[1], Eman T. Alharbi[1], Aisha M. Alshiky[1], Saja S. Alqurashi[1], Jayaprakash Kar[2]

[1]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
[2]Department of Information Systems, Information Security Research Group, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA
Email: jayaprakashkar@yahoo.com

Received 27 September 2014; revised 25 October 2014; accepted 20 November 2014

Abstract

E-mail security becomes a critical issue to research community in the field of information security. Several solutions and standards have been fashioned according to the recent security requirements in order to enhance the e-mail security. Some of the existing enhancements focus on keeping the exchange of data via e-mail in confident and integral way. While the others focus on authenticating the sender and prove that he will not repudiate from his message. This paper will survey various e-mail security solutions. We introduce different models and techniques used to solve and enhance the security of e-mail systems and evaluate each one from the view point of security.

Keywords

E-Mail Security Enhancement, Malware Attacks, Authentication, Integrity

1. Introduction

Nowadays, most of people and organizations use the e-mail for different needs to exchange the information between users. E-mail application is the important network applications. It is significant when business, health and educational communities use it for exchange of critical information such as business information, health patient record and so on [1].

Recently available e-mail standards provide protection of e-mail messages using standard cryptographic techniques and formats like PGP S/MIME [2]. But these standards focus on the protection of e-mail contents by performing series of cryptographic mechanisms rather than the header of e-mail. Accessing one's e-mail account

How to cite this paper: Babrahem, A.S., Alharbi, E.T., Alshiky, A.M., Alqurashi, S.S. and Kar, J. (2015) Study of the Security Enhancements in Various E-Mail Systems. *Journal of Information Security*, **6**, 1-11.
http://dx.doi.org/10.4236/jis.2015.61001

does not occur from only one particular device, often from many different ones, which causes an increase in the risks of unauthorized access, eavesdropping or altering the user messages. For this issue, it is very significant for user privacy and accuracy to assure the authenticated and confidential use of e-mail while moving in a public environment or with public transport [2].

Usually, the authentication systems depend on some parts of information (password), physical property of the individual (biometrics), or some derived property (tokens). The user is considered authenticated if the authenticating system can verify that the shared secret key was presented correctly. This shared secret key is required to be encrypted in order to offer confidentiality which secures it from being sniffed by hackers. Moreover, a message digest should be performed also to assuring the integrity of the message's contents. When both confidentiality and integrity are combined, non-repudiation will be assured. In order to secure the data transmission process, the security of the authentication process should be observed and make sure the data is encrypted and decrypted in the correct way because there are many malware attacks which can infect the system [3].

Current e-mail system has many serious problems and the most important are the following [3]:

- The authentication mechanism that based on user name and password considered very weak because attacker can easily guess password using dictionary attack and break authentication mechanism.
- Protection of mailboxes and e-mail messages on mail servers depend on Operating Systems (OS) security. If OS security is not properly configured and policies are not enforced, then attacker can easily gain access to these Mailboxes and e-mail messages.
- Most of e-mail users send e-mails in clear, because they don't have sufficient knowledge to configure security parameters. So, attacker can easily read and modify e-mail letters.
- Most of current e-mail systems don't handle attachment files in conventional and inefficient way.
- Most of e-mail clients and servers do not support effective mechanism for confirmation of delivery of e-mail letters.

Because of the increase in the use of the computer technologies day by day in personal and institutional spaces, it is necessary to use the e-mail security systems efficiently. E-mail security is the process of protection from unauthorized access to information, its use, revelation, destruction, change and harm. Information privacy, integrity and accessibility are the main elements on which e-mail security is based [4]. In this paper we introduced different models and techniques used to solve and enhance the security of e-mail systems. We perform a comparison between these solutions in order to find which one of them is giving the best level of security. This paper is divided as the following: Section II includes a background about the existing techniques used to handle the security of e-mail systems; Section III introduces the various enhancements that applied to the security of e-mail systems, which are divided into three subsections according to the enhancement that provided.

2. Background

The early e-mail systems were very simple. It just includes the basic e-mail functions without any security services [5]. Nowadays most of people and organizations use the e-mail for different needs to exchange their sensitive information. As a result, the existing e-mail systems were developed to be more advanced to accommodate user's needs. However, the e-mail systems become the target to many threats and eavesdroppers [6]. For that, the need for high-secured e-mail systems and applications increased. Accordingly, it is necessary to define new properties toward enhancing the e-mail security and then the security services that implement those properties in the e-mail systems need to restructure. These enhancements include:

1) E-mail Message Confidentiality.
2) E-mail Message Integrity.
3) Message sender Authentication.
4) Message sender Non-Repudiation [5].

There are different security techniques defined in order to implements these properties. The most talented techniques used are the Encryption and digital signature. Encryption used to verifying the data confidentiality whereas the digital signature verifies the rest of enhancements (e.g. Integrity, Authentication and Non-Repudiation [5] as illustrated in **Figure 1**.

There are many protocols proposed to offers the Encryption together with the digital signature and the most famous existing ones are the PGP (Pretty Good Privacy) and S/MIMI (Secure/Multipurpose Internet Mail

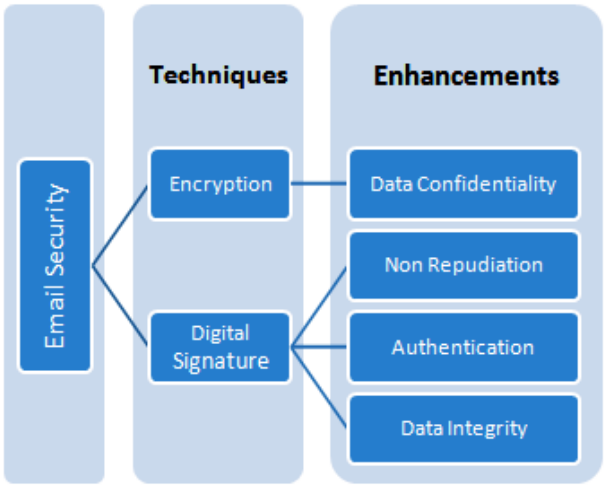

Figure 1. Security techniques and enhancements.

Extension). Both PGP and S/MIMI are used to provide the e-mail with many security services such as data confidentiality and sender authentication [5] [8] [9].

These protocols offer the confidentiality by encrypting the e-mail message using one of the public-key cryptography algorithms. For PGP, CAST, IDEA, or 3DES algorithms are used for encryption/decryption whereas the S/MIMI uses El-Gamal cryptographic algorithm [8] [9] [11] [12].

According to authentication, The PGP and S/MIMI append digital signature into the encrypted message to provide the sender authentication. PGP uses the SHA-1 algorithm to calculate the Hash value while, S/MIMI uses the same algorithm for the hash value but MD5 algorithm it required in the receiver end to support the compatibility with previous versions. After calculating the hash value, both PGP and S/MIMI encrypt it with the sender private key using the RSA or DDS algorithms [8]-[10]. S/MIME can regard as standard for industry and then it is suitable for used in the organization and commerce. In the other hand, PGP is used by individuals for securing the personal e-mails [9].

3. Enhancing the Security of E-Mail Systems

Some of recent solutions which are proposed to improve and enhance security e-mail discussed in this section in more details and each solution classified according to which enhancement provided by it. Some of these solutions include a particular enhancement such as authenticated e-mail systems and the confidentially and Privacy e-mail Systems. Some enhancements, such as integrity and non-repudiation, needs to integrated with other enhancements to provide the solution with high level of security. The classifications of proposed solutions clarified in next subsections and **Figure 2** illustrated the general classification of this study.

4. Authenticated E-Mail Systems

Even with the maturity of today's e-mail infrastructure, it is complicated to ensure the authenticity of a sender address for in bound mails. For that, the developing of e-mail sender authentication mechanism as a promising way to verify identity of the senders has attracted researchers over the years. E-mail sender authentication mechanisms enable receivers to automatically differentiate forgeries from authentic messages. There are number of system which proposed in different works that designed to verify authenticity of a sender address and to make spasm e-mail hard to exist [13].

The main vulnerability in Simple Mail Transfer Protocol (SMTP) is that users are not authenticated, which allows the spoofing attacks. A Model has been proposed [13] to enhance e-mail authentication and preventing e-mail address spoofing and to overcome SMTP authentication vulnerability. The proposed solution works by authenticating the domain of the sender. It obtains the sender host's information by checking the information of the "Received" field for an e-mail in the user side to distinguish if it is a spooled e-mail or not. The methodology of the proposed enhancement displayed in **Figure 3**, and it works as the following:

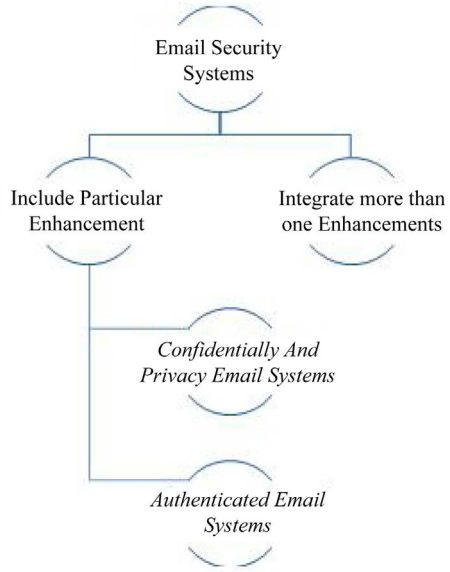

Figure 2. Survey classification.

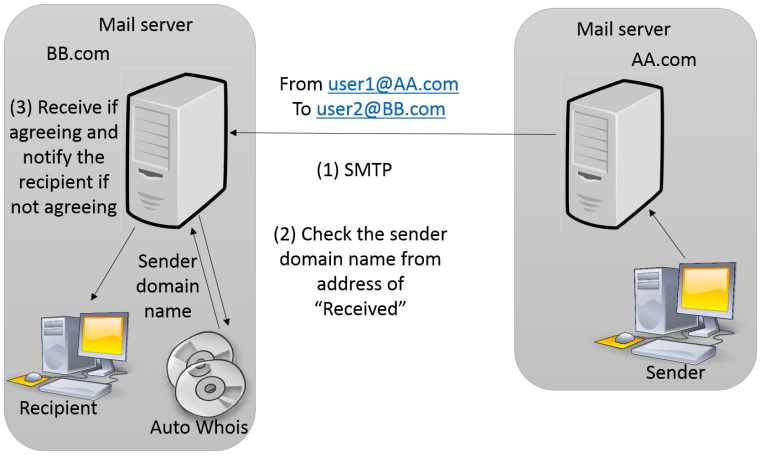

Figure 3. Authentication of the sender domain.

- The mail server of A.com will connect to the e-mail server of B.com via SMTP.
- The sender domain name is obtained through the mail server of b.com from IP address that placed in "Received" field.
- Comparing the sender domain name which obtained in "2" with the one which found in the form field. If they are the same, then the authentication succeeds. Otherwise, the sending of e-mail is failed and the recipient will informed.

The outcome of the proposed work reached the objectives of authenticating the e-mail address and preventing various address attacks such as the address spoofing and man in the middle attack and other solution introduced, iSATS is a crypto-based e-mail sender authentication system that work on the SMTP envelop, in particular on MAIL FROM: command, to do domain level authentication through the SMTP time. iSATS requires establishment of a trusted authority (TA) also known as private key generator (PKG), responsible for issuing the secret key (SK) and system parameters and responsible to verify the identity of a domain before SK issuing. The process of iSATS can be divided into four steps

- system setup: executed only one time at the start to create whole identity based public key cryptography (IBC) environment by a TA. The results of this setup generation of Master Key (used to generate SK) and System Parameter which are publicly available.

- Identity Verification and Secret Key Extraction: when any domain wants to become part of iSATS and request a SK. First, TA verify domain identity. After that, the TA issue system parameters and a SK corresponding to domain name(unique). **Figure 4** illustrate the process of domain joining iSATS.
- Signature Generation: executed when a user want to send an e-mail. iSATS requires the sender's Mail Transfer Agent (MTA) to generate a signature on the sending user's e-mail address alice@example.com) using the SK and system parameters of the domain. Then the signature is appended to MAIL FROM: SMTP envelop.
- Signature Verification: the MTA on the receiving side will verify the signature after receiving the MAIL FROM: command by using the public system parameters, signed text *i.e.* sending user's e-mail address from MAIL FROM, signature (extracted from MAIL FROM:): and the domain name of the sender. **Figure 5** illustrate E-mail Processing with iSATS. iSATS using IBC to leverages identity based signature (IBS) and compared to traditional public key cryptography IBC saves the burden of managing and distributing the public keys, since publicly available unique identities are used as public keys. Also, iSATS can be integrated with tools generally used with e-mail infrastructure; this allows an incremental deployment of iSATS. The potential bottlenecks of iSATS are the computationally expensive tasks, specifically the extraction of SKs by the TA and the signature generation and verification. Through implement iSATS, there is performance with low processing overhead on different systems.

Other solution proposed [15] to provide authentication mechanism for e-mail which is client-oriented Secure Socket Layer (SSL)-based anti-spoofing application. It provides users with a table of user details (Internet Protocol (IP) addresses and the names of users on the subnetwork). It uses cryptographic self-signed certificates to exchange a secure authentication message alongside the e-mail with a view to prevent spoofing. For send e-mails, the application connects to mail servers. If the connection is established, the e-mail address and the password of the user is confirmed using an authentication class. If the validation process is doing well, the e-mail will send to any recipient. When a user needs to send e-mail to another user, the user's name can be selected from the table. If the name is selected, the IP address is automatically stored to sending an authenticated message by setting up a secure Transport Control Protocol (TCP) connection using SSL. The proposed architecture for the application is illustrated in **Figure 6**.

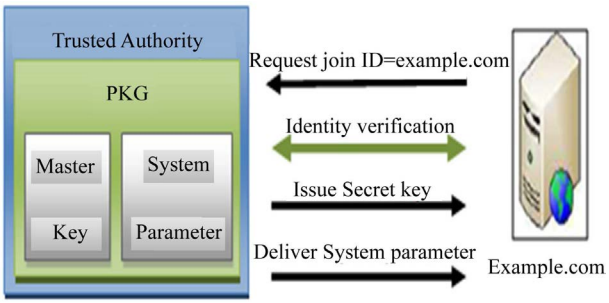

Figure 4. Process of domain joining iSATS [14].

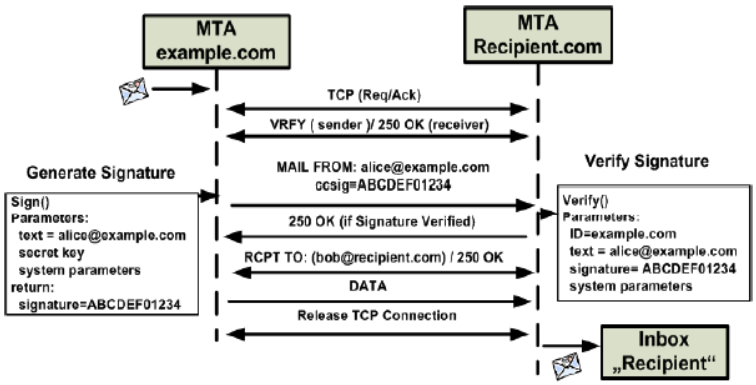

Figure 5. E-mail processing with iSAT.

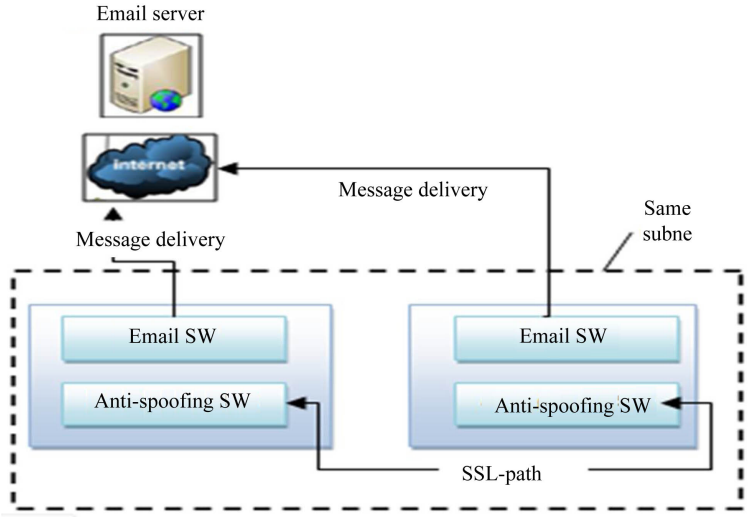

Figure 6. E-mail Architecture with anti-spoofing application [15].

The advantages of this application are the incorporation of SSL, its ability to allow users to use anti-spoofing measures independently of any e-mail server and its user-friendliness. While one limitation of the program is that in order to receive a confirmation message, the client computers have to be turned on and the application should already be running.

5. Confidentially and Privacy E-Mail Systems

The protection of data on transactions and privacy of user information is a key of interest for users. Based on this motives Ioannis *et al*. [2] proposed secure e-mail system to provide privacy of locations from which e-mail system is accessed, protection of e-mails, and legitimate users authentication. This system considers several principles in terms of user friendliness, usability, scaling, privacy of users, and security of e-mails. The process of Secure e-mail proxy interactions can be divided into four steps as shown in **Figure 7**.

- **Step 1**: The user logs into the secure e-mail proxy using the e-mail address and password of his/her native e-mail system.
- **Step 2**: For new users, the proxy generates a key pair, sends public key to the CA server, receives and stores the user's certificate.
- **Step 3**: The proxy fetches via IMAP the e-mails from the corresponding e-mail server. Upon double click, each letter is cryptographically processed and displayed.
- **Step 4**: The user can now send signed and encrypted e-mails.

Other solution proposed [2] to provide secure, high assurance and very reliable e-mail system that is CryptoNET. This system handles standard e-mail security services like signed and encrypted e-mail. In addition, it provides many extended security features. The concept of proposed secure e-mail system is the using of proxy-based architecture to provide extended security features and make the system interpretable with existing standard e-mail systems. The proxy server, Secure e-mail Machine (SEM) server is located between SEM client and standard e-mail server as show in **Figure 8**. At initial activation, SEM client either generates self-signed certificates or it requests them from a local Certification Authority (CA) to provide strong authentication and secure communication between sender and receiver. Moreover the SEM client protected the address book by encrypting it with symmetric key. This system protects the e-mail letters based on S/MIME. In this case, encapsulated attachments into signed and/or use public-key cryptography standards PKCS7 objects by SEM client then uploads these attachments to the SEM server. Then sends back a URL corresponding to each attachment file by SEM server. Then SEM client add URL(s) into the body of an e-mail message prior to its sending. At the recipient's side the SEM client parses the body of a message and extracts URL(s). Then SEM client download files from received URLs then decrypts them before display. This proposed system has a limitation that is the proxy server represents a single point of failure.

In order to handle the cryptographic key management, a Trusted e-mail System has been proposed in [16]

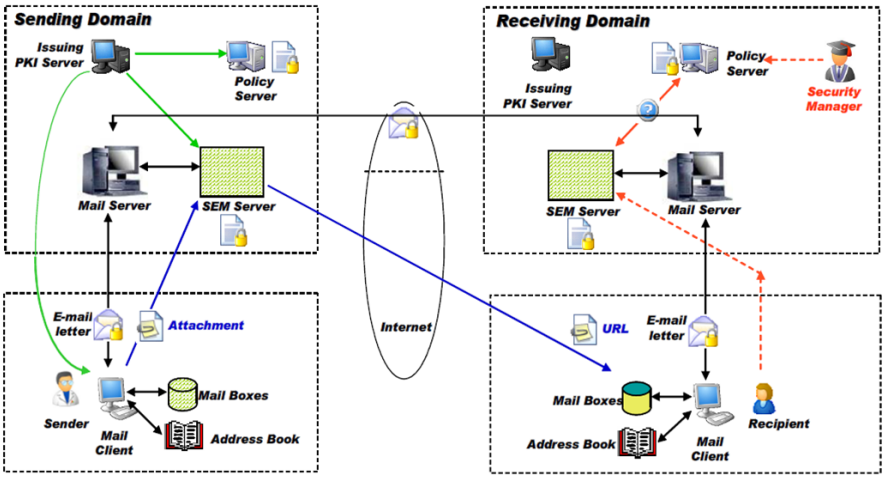

Figure 7. Secure e-mail proxy interaction [16].

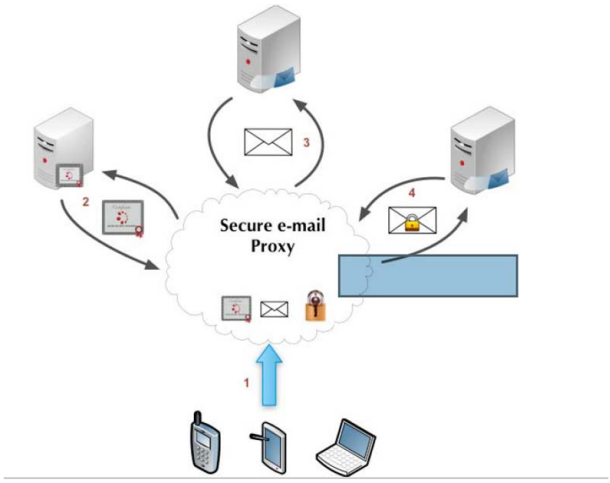

Figure 8. Architecture of Secure e-mail and communication with SEM client and SEM [2].

using different technique. This system uses hardware-based cryptographic functionality of the Ephemerizer and Trusted Platform Module (TPM) concept. TPM authenticate the users by using hardwares keys, which used also for e-mails encryption. The Ephemerizer provides ephemeral keys and manages their expiration time, so the message becomes unreadable after they expire. By applying these technologies together, the cryptographic keys will managed securely and nobody can read e-mails other than the intended users. In this system, the exchange of e-mails has done after authenticating the sender and receiver by using TPM. This is done by the creation of Attestation Identify Key (AIK) and Endorsement key (EK) by each agent and then certifies them with a privacy certificate authority (CA) [7]. Now, each agent can prove that it has a TPM. Then the sender can send the message by following these steps:

- The sender set the expiry date for his message. He will receive pair of public keys, the EP_{pub} from the Ephemerizer and $AIKECR_{pub}$ from AIK. The sender will encrypt his message by a secret key s. This secret key encrypted twice, first encrypted using the $AIKECR_{pub}$. Then it encrypted with the EP_{pub}.
- When the recipient receives the encrypted message, the receiver sends the encrypted secret key s to the Ephemerizer.
- The Ephemerizer extract the ephemeral key used in the encryption process of the secret key s and checks its expiration date. If it is still not expired, the Ephemerizer decrypts s with the private key EPprv and sends it to the receiver. Otherwise, the message cannot recovered. Then, the receiver decrypt s by using private key of AIK $AIKEC_{Rrv}$. Now the secret key is decrypted twice and can be used to decrypt the message. This trusted

e-mail security can be used over a paid service, and it did not implemented in the free services.

6. Integration of E-Mail Security Enhancement

The need for high-secured e-mail systems and applications increased [6]. And as mentioned in the previews subsections, some of the e-mails systems provide a particular security enhancement to the e-mails such as authentication or privacy and confidentiality. But there are numbers of environments which are need to Integrate more than one security enhancements in one e-mail system to improve its security significantly and protect the e-mail systems from different flaws. In this section, we will mention two different e-mail systems which integrated two or more security enhancements to provide higher level of security. The proposed e-mail security system in [1] is a complete end to end system used the improved encryption/decryption algorithm integrated with the user's thumbprint biometric features. This system state a multilevel scale for the security with three different levels: high, average and low. The level selection depends on the sensitivity of the message. In order to ensure the confidentiality of the e-mail message plain text, the encryption/decryption algorithm in the proposed system consists of four steps: use of the XOR ciphering, message reversal, Use the AES algorithm with 256-bit length key and the addition of some extra security parameters (such as: date/time, security level, random and dummy numbers). The biometric features used to ensure the authentication between the e-mail sender and receiver. The sender attached his ID and fingerprint template with the encrypted messages. The receiver cannot be decrypted the message without a valid sender's ID and fingerprint template. The proposed system [1] is examined and proved its effectiveness on the Gmail server. The good point for this proposed security system is its suitability to be used with any other biometric identification type. There is one disadvantage for this system which is, the exponential relationship between the time used for the encryption/ decryption and the plain text size as in **Figure 9**.

SAHASTRADHARA application [6] designed to offers the e-mail security from the client side in pluggable mode to work with MS Outlook server. It provides e-mails with the essential security feature such as, data confidentiality and integrity and authentication and non-repudiation of message source. SAHASTRADHARA used Symmetric block ciphering algorithm in order to provide the confidentiality. It characterized as high secure, fast, compact and easy algorithm. The integrity is obtained in this application by using the SHA-1 and RSA. Where the Non-Repudiation achieved by using the bi-directional digital signature which encrypt the hash value twice using the RSA, first time by the sender private key and then by the receiver public key. The user keys and digital certificates are securely stored in the E-Token. SAHASTRADHARA used three authentication techniques. It used the password to validate the e-mail account. Also, it used the Biometric authentication (finger print) to validate the user when viewed or send any e-mail. Moreover E-Token authenticates the user but it must be inserted to the user's computer before sending or viewing any e-mail.

The only limitation of this system that it is E-Token based system but the system can be initiated before inserting the E-Token and it may led to some security problems. Following table illustrates and summarizes each solution with its provided security level and its limitations.

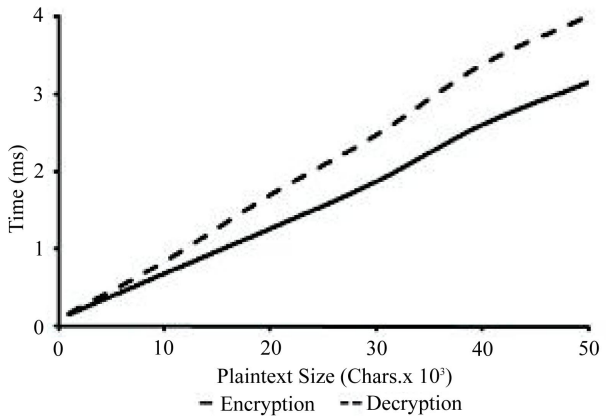

Figure 9. Relationship between encryption/decryption time and the plaintext size [15].

7. Future Works

According to this survey, we found that the future researches in the e-mail security field are directed to set up a highly efficient security system in which the following are available:

1) Assuring the truth identity of the e-mail's user to prevent the unauthorized access and different attacks.

2) Encapsulating the messages by applying multiple levels of encryption to ensure its confidentiality and prevent any modification on it.

3) Protecting e-mails transfer from sender to receiver via secure channel.

4) Applying a mechanism on the sent e-mails that destroy the message in case the work of several attempts to decrypt it.

5) Applying client-side security system to provide more of restrictions and to make effective and securely transactions even if the security of server harmed.

6) There are a lot of environments such as cloud computing, mobile and so on which use the e-mail systems. So the security requirement of especial environment should be taken in consideration and appended with e-mail security requirements.

8. Conclusion

The e-mail system security is one of the most important trends that should be taken into account within these days when transferring the data, especially for those which require a confident and authenticated communication mean. In this study, we introduced various techniques that are used to enhance the security of the e-mail systems. The main enhancements are founded in two directions, which are the authentication of the e-mail user identity and the confidentiality and privacy of the e-mail transforming. We show that these enhancements have improved the performance of the proposed systems and they reached the required level of security. In **Table 1**, we summarize a comparison between the proposed systems according to their level of security, and figured out the limitations of each system in order to execute them in a future work.

Table 1. Comparison and limitation of the proposed systems.

Schemes	Security level	Limitations				
heading Vikas *et al.* [13]	Authenticate the identity of the e-mail sender	The distribution of public key is				
	by checking the header field of the message	a legitimate binding to its owner.				
Hameed *et al.* [8]	Authenticate the identity by providing signature	iSAT has low computational footprints				
	to provide easy and reliable approach to combine	footprints and overhead is imposed.				
	the legitimate sender identity unambiguously to					
	his e-mails					
Mooloo *et al.* [14]	Provide authentication by using cryptographic	To receive a confirmation message				
	self-signed certificates for exchange a secure	to the client computers have to be	authentication message alongside the a e-mail	turned on and the application should	with already be running vision to avoid spoofing.	already be running
Kounelis *et al.* [15]	Protection of e-mails, privacy of locations from	The proxy server represents a single				

Continued

	which the e-mail system is accessed, and	point of failure, when it is fail, we need Implementation issue that is complicated to overcome is the native security policies of the different e-mail servers a processing overhead emphasized that encrypting a e-mail does not allow a third party to see the content.	authentication of legitimate users.	a backup.
Ghafoor *et al.* [2]	Enhance e-mail system using certificates, smart Cards and crypto objects with high degree of Security for professional users.	The proxy server represents a single point of failure, when it is fail we need a backup.		
J. Jang *et al.* [16]	Trusting both parties according to their TPM Message.	(paid	key then make a triple encryption transferred	services
Al-taee *et al.* [1]	Ensuring the confidentiality of the email message plaintext using improved encryption authentication between the email sender and receiver using biometric features.	Exponential relationship between the time used for the encryption/ decryption and	and decryption algorithm and ensuring the	the plaintext size
Shukla *et al.* [9]	Provides e-mails with confidentiality by using Symmetric block ciphering algorithm. The integrity is provided using the SHA-1 and RSA. It uses three authentication techniques: password, Biometric authentication and E-Token, to validate the e-mail account and the user. Non-Repudiation achieved using the bi-directional digital signature.	The system can be initiated before inserting the E-Token		

Acknowledgements

We would like to thank to our supervisor Dr. Jayaprakash Kar for his valuable suggestions and comments that helped improving this work. This support is greatly appreciated.

References

[1] Al-taee, M.A., Al-Hassani, H.N., Bamajbour, B.S. and Al-Jumeily, D. (2009) Biometric-Based Security System for Plaintext e-Mail Messages. *Second International Conference on Developments in eSystems Engineering* (*DESE*), Abu Dhabi, 14-16 December 2009, 202-206.

[2] Ghafoor, A., Muftic, S. and Schmölzer, G. (2009) CryptoNET: Design and Implementation of the Secure Email System. *Proceedings of the* 1*st International Workshop on Security and Communication Networks* (*IWSCN*), Trondheim, 20-22 May 2009, 402-407.

[3] Al-Saadoon, G.M.W. (2011) Authentication and Virus Detection Enhancement for Client and Server Applications. *Journal of Emerging Trends in Computing and Information Sciences*, **2**, 390-395.

[4] Baykara, M. and Das, R. (2013) A Steganography Application for Secure Data Communication. *International Conference on Electronics, Computer and Computation* (*ICECCO*), Ankara, 7-9 November 2013, 309-313.

[5] Cailleux, L., Bouabdallah, A. and Bonnin, J.-M. (2014) Building a Confident Advanced Email System Using a New Correspondence Model. 28*th International Conference on Advanced Information Networking and Applications Workshops* (*WAINA*), Victoria, 13-16 May 2014, 85-90.

[6] Shukla, R., Prakash, H.O., Bhushan, R., Venkataraman, S. and Varadan, G. (2013) Sahastradhara Biometric and EToken Integrated Secure Email System. 15*th International Conference on Advanced Computing Technologies* (*ICACT*), Rajampet, 21-22 September 2013, 1-4.

[7] Kar, J. (2014) Provably Secure Online/Off-Line Identity-Based Signature Scheme for Wireless Sensor Network. *International Journal of Network Security*, *Taiwan*, **16**, 26-36.

[8] Hameed, S., Kloht, T. and Fu, X.M. (2013) Identity Based Email Sender Authentication for Spam Mitigation. *Eighth International Conference on Digital Information Management* (*ICDIM*), Islamabad, 10-12 September 2013, 14-19.

[9] Stallings, W. (2014) Electronic Mail Security, in Cryptography and Network Security Principles and Practice. 6th Edition, Pearson Education, Upper Saddle River, 591-615.

[10] Kar, J. and Majhi, B. (2009) An Efficient Password Security of Three Party Key Exchange Protocol Based on ECDLP. 12*th International Conference on Information Technology* 2009 (*ICIT* 2009), Tata McGrow Hill Education Private Limited, Bhubaneswar, 75-78.

[11] Kar, J. and Majhi, B. (2009) An Efficient Password Security of Multiparty Key Exchange Protocol Based on ECDLP. *International Journal of Computer Science and Security* (*IJCSS*), **3**, 405-413.

[12] Kar, J. and Majhi, B. (2009) A Secure Two-Party Identity Based Key Exchange Protocol based on Elliptic Curve Discrete Logarithm Problem. *Journal of Information Assurance and Security*, **5**, 473-482.

[13] Zadgaonkar, S., Pandey, V.C. and Pradhan, P.S. (2013) Developing a Model to Enhance E-Mail Authentication against E-Mail Address Spoofing Using Application. *International Journal of Science and Modern Engineering* (*IJISME*), **1**, 13-17.

[14] Mooloo, D. and Fowdur, T.P. (2013) An SSL-Based Client-Oriented Anti-Spoofing Email Application. *AFRICON*, Pointe-Aux-Piments, 9-12 September 2013, 1-5.

[15] Kounelis, I., Muftic, S. and Loschner, J. (2014) Secure and Privacy-Enhanced E-Mail System Based on the Concept of Proxies. 37*th International Convention on Information and Communication Technology, Electronics and Microelectronics* (*MIPRO*), Opatija, 26-30 May 2014, 1405-1410.

[16] Jang, J., Nepal, S. and Zic, J. (2008) Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries. 8*th IEEE International Conference on Computer and Information Technology*, Sydney, 8-11 July 2008, 402-407.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.