Enhancement of Email Security Services

Fatima Aziz Rawdhan, Mahmood Khalel Ibrahim

Abstract—One of the most important services in the Internet is the E-mail Service. The E-mail server can be vulnerable to several types of cyber-attacks. The aim of this research is to analyze and improve the E-mail service. The proposed system is a hybrid cryptosystem that use public key to transfer the secret key (Ks) and the symmetric cryptosystem to ensure the system confidentiality, integrity and authenticity. Security service in the proposed system based on examining the user ID, which is associated with a strong password to resist the brute-force attacks. The second service is the secret key exchange, where the encryption protocol uses Public key to encrypt and transfer the secret key (Ks), The third service is Confidentiality and Integrity, the asymmetric encryption is used to sign and encrypt the message. The protocol offers some security services options, which are available for the user's requirement. The system and its tools were designed and developed using Visual Basics, Apache and database MySQL.

Index Terms— E-mail, Authentication, Encryption, Integrity, Security Services.

IJSER

1 INTRODUCTION

In the present time E-Mail is the most widely used communication system in daily life and very important. Regardless of the geographical distances; the major cause for using E-Mail is probably the convenience and speed which it can be transmitted the message in E-Mail system [1].

E-Mail system has many protocols, which used to achieve a particular function in the process of sending or receiving E-Mail messages. The commonly used E-Mail system protocols are SMTP for sending and POP or IMAP protocol for retrieving E-Mail messages [6].

In any Email System, the users require a type of software interface that enables them to interact with the server of the email system and in addition allows them to compose, send, store, and read messages. That software interface is called the mail client, which it can be a desktop application such as, Mozilla Thunderbird, MS outlook, or web-mail [5]. One of the dangerous problems observed in mail clients is its lack of security. In addition, the email messages send across the internet is not protected as it might be not delivered or read by unauthorized individuals. Currently all mail clients supply authentication through a username and password, which is vulnerable to attacks as the passwords, could be easily hacked [2].

Three basic needs are considered essentials for data security; the confidentiality, Availability, and Integrity. The protection of data from the unauthorized access is ensured by the confidentiality, while the recovery from the hardware, and software errors, or the malicious activity is provided by the availability. Finally, unauthorized users are prevented from the inappropriate modification through the use of Integrity [3].

2 THREATS OF E-MAIL

There are many types of E-Mail security threats, such as the following:

1. **Viruses**: Viruses are threats that are most high risk and publicize of all issues. They often deliver fatal load, bringing down the whole mail system, and destroying data, as a result they are very dangerous [8].
2. **Spam:** Spam or junk mail refers to the process of sending email to specific number of people for advertising purposes or malicious intent. The target of the spam is often lists that are created by the searching of the data from the Internet [7].
3. **Phishing:** It is considered as one of the most popular attacks of email. Originally, it is the type of attack that thieves the user's confidential information like passwords [9].
4. **Man-In-The-Middle-Attack**: The man in the middle attack happen when an attacker inserts himself between two parties and pretends to be one of the parties [8].
5. **Eavesdropping**: E-mail messages pass through networks, which are part of whole picture. Therefore, it is very easy for someone to track or capture your message and read it [7].
6. **Data diddling:** This type of attack occurs when the attacker changes the data, while routing between communications peers [8].
7. **Dictionary attacks:** The attacker in this type of attack can choose a common used password then trying them until the he can discover the right password [8].
8. **Denial of service attack:** occurs in the time the system receiving many requests that cannot return communication with the requestors[8].

3 PROPERTIES OF SECURE OMMUNICATION

The following properties are regarded as a main secure communication properties:

1. **Confidentiality:** used to prevent the disclosure of information to unauthorized [12]. Only the sender and receiver are able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, it's requires that the message be somehow encrypted so that an intercepted message cannot be understood by an intruder [11].
2. **Message Integrity:** that the same message/data should arrive at receiver end as it can be send by sender. No alteration intentionally or accidentally takes place during transfer [10].
3. **End-point Authentication:** Both the sender and receiver must be able to confirm ID of the other party involved in the communication, to confirm that the other party is really who or what they claim to be [10].
4. **Availability**: information must be available when it is needed. This means that the computer systems used to process and store the information, the security controls used to protect it, and the communication channels used to access it must be operating correctly [12].

4 E-MAIL SECURITY PROTOCOLS

E-mail security protocol is in charge of protecting the email messages and passwords. It assures the privacy of the clients. Some Providers of E-mail are supporting a secure mail protocol. The TLS prevents the spoofing and eavesdropping between email servers, it is used for providing privacy over the Internet and authentication of the end user. Separate protocols are used to provide email messages' security such as PGP and S/MIME [13].
Two protocols can be used in order to make the previous defenses, and to provide the E-mail security functions related to the message integrity, confidentiality, authentication, and the non-repudiation; those are the PGP and S/MIME [8].

4.1 Secure/Multipurpose Internet Mail Extension (S/MIME)

S/MIME is considered one of the security protocols, that is basically designed for providing E-mail security. This protocol is considered as an enhancement of the MIME which is the Multipurpose Internet Mail Extension (MIME) protocol [13].
S/MIME provides authentication (digital signatures) and confidentiality (encryption). S/MIME is not a special software product but a standard designed to be implemented by various E-Mail vendors, so that any two S/MIME-supporting mail clients can communicate securely [14].

4.1.1 S/MIME problems

A. The adoption of S/MIME is still considered hard because of the complexity of public key cryptography and usability problems of email clients which are supporting S/MIME [8].
B. Second limitation with S/MIME is its inability to ensure non-repudiation through keys in situations where keys are lost [15].

4.2 Pretty Good Privacy (PGP)

PGP can be defined as a public key cryptographic package and its usage is intended for the public use. All the authenticity, integrity, confidentiality, and non-repudiation of the sender can be provided by the PGP. In spite of it can encrypt any files or data; it is also used for the non built-in security email as originally implemented [16].
Encryption of the message content happens directly on the user device, through the use of the public key of the receptionist's. In order to ensure that the message contents have not been change during transmission, a message can be digitally signed. Message signing happens at the moment of sending and is signed by a unique Private Key of a sender. Verification happens on the recipient's device with a sender Public key and no passphrase is required for signature verification [4].

4.2.1 PGP Problems

A. Many problems are associated with PGP, one of them is the management process of keys and this is considered one of the biggest challenges in PGP. The cryptography of the public key needs the sender to gain the public key of the receiver beforehand, so as to be able to start the encrypted communication of PGP [17].
B. PGP is suffering from many types of problems such as the weakness in encryption and low performance [13].

5 PROPOSED E-MAIL SECURITY PROTOCOL

A protocol of E-Mail security is proposed by [4]. The proposed protocol considered as s prototype protocol that uses public key cryptography to encrypt a secret key (Ks) of the sender and send it in secure method to the recipient, and uses generated Ks to sign and encrypt the message to ensure Integrity and Confidentiality. Authentication and non-repudiation are preserved by sending random number (Nonce) to both sides; the server and the recipient. The protocol consists of the following two stages [4]:

1. The first stage comprises of client's registration and sending their ID and public keys to the E-Mail server and this to be done once.

2. The second stage starts when a registered client wants to send a message to any other registered client. The second stage includes requesting public key of the recipient and performs the required security services (Integrity, Confidentiality), and secret key encryption. The second stage ends with receiving recipient's receipt of reception from the recipient to the sender. For more details refer to [4]. Fig.1 illustrates the architecture of proposed protocol.

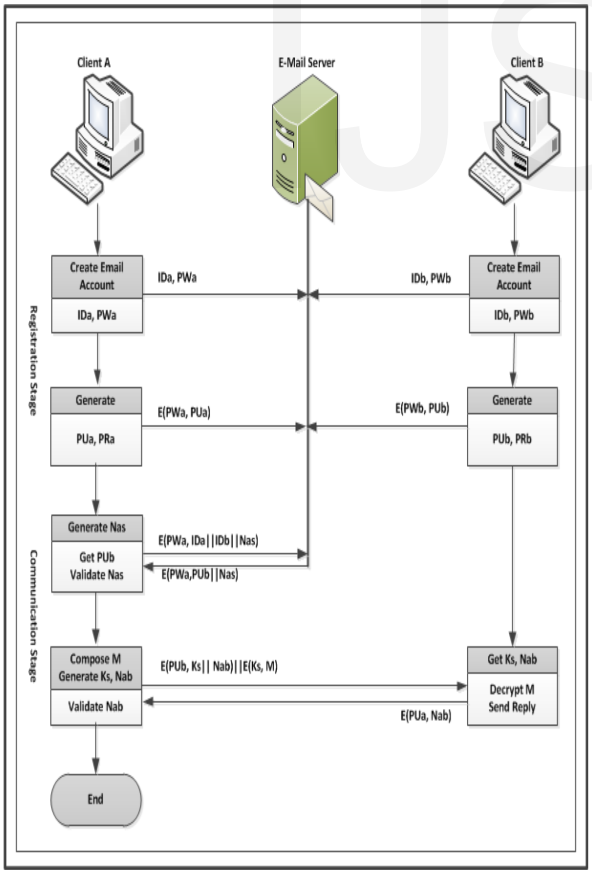


Fig. 1. Proposed Secure E-Mail Protocol [4].

6 ENHANCEMENT OF THE PROPOSED E-MAIL SECURITY PROTOCOL

In this paper, an enhanced version of the proposed protocol discussed in section 4 is presented. . Through studying and analyzing the proposed E-Mail security protocol, some enhancements have been made to overcome the drawback and vulnerabilities of the protocol and to increase its performance and strengthen it's security. Enhancements can be described as follow:

1. In the first step, user registration, the user should not send his username and password to the server without encryption. Encryption of registration information will protect the system from any eavesdropping attack conducted to obtain any information to penetrate the system.
2. The second improvement in the proposed protocol stated (in step 1.2 - below), where the public and private keys get generated, then the user/client request the PUs from the server to use it to send his own details (user name, password and the public key), all encrypted by the PUs. While the proposed protocol suggests encrypting the information using the user's password, and this procedure is not practical to apply.
3. The third improvement (add-on) to the proposed protocol is the login stage (in step 2-below), where the user/client must use the user name and password, which were previously sent to the server (as encrypted) during the Registration Stage. This procedure has been added in order to protect the system from unauthorized users to enter the system.
4. The proposed protocol suggests exchanging the massages/emails directly between the end-users (email clients) without using any database storage, and this is not adequate for standard emails systems. Therefore, this protocol can be improved by adding database storage, to host the emails data until the far-end users retrieve them.

Fig. 2 demonstrates improved architecture of the enhanced protocol.The improved proposed protocol is listed below:

Symbols	Notation
||	Concatenation
A, B, … N	Clients
CM	Ciphered Message
D	Decryption Process
E	Encryption Process
ID_i	Identifier of client i
K_s	Secret Key

IJSER

M	Message
PR_i	Private Key of client i
PU_i	Public Key of client i
PW_i	Password of client i
S	E-Mail Server
SG	Sign Massage
SM	Signed Message

1. **Registration Stage (All Clients Create E-Mail Account)**

1.1. Create Account (All Clients Create Accounts)

1.1.1. A: generate ID_a, PW_a

1.1.2. B: generate ID_b,PW_b

....

1.1.3. N: generate ID_n,PW_n

1.2. Initialization (All Client Generate Public Key Pair)

1.2.1. A: generate PU_a,PR_a

1.2.2. B: generate PU_b,PR_b

....

1.2.3. N: generate PU_n,PR_n

1.2.4. A: S (A Request PU_S from Server)

1.2.5. S: A (Send PU_s)

Then:

1.2.6. A→S: E(PU_s,ID_a||PW_a||PU_a)

1.2.7. B→S: E(PU_s,ID_b|| PW_b||PU_b)

....

1.2.8. N→S: E(PU_s,ID_n||PW_n||PU_n)

2. **Login Stage (Any Client Login E-Mail Account)**

2.1. A→S: E (PU_s, ID_a || PW_a)

2.2. S: D (PR_s, ID_a|| PW_a)

→ verify ID_a and PW_a and send response to client A

2.3. B→S: E (PU_s, ID_b || PW_b)

2.4. S: D (PR_s, ID_b || PW_b)

→ verify ID_b and PW_b and send response to client B

....

2.5. N→S: E (PU_s, ID_n || PW_n)

2.6. S: D (PR_s, ID_n || PW_n)

→ verify ID_n and PW_n and send response to client B

If client already existing in the server, the client, opens Email GUI and requests a new E-mail.

Then

2.7. S →A: E (PU_a, ID_b ||ID_c.... ID_n)

3. **Communication Stage**

3.1 A: S (A request PU_b from Server)

3.1.1 A: generate N_{as}

3.1.2 A→S E(PW_a,ID_a||ID_b||N_{as})

3.1.3 S→A E(PW_a,PU_b||N_{as})

3.1.4 A D(PW_a,PU_b||N_{as})

→get PU_b,verify N_{as} ?

3.2 A: S (A send Message to B)

3.2.1 A: compose M, generate K_s, N_{ab}

3.2.2 Integrity? MS=SG(K_s,M)using MD5

3.2.3 Confidentiality? MC=E(K_s,M) using AES

3.2.4 A→S E(PU_b,K_s)||E(K_s,N_{ab}) ||E(K_s,M)

And store in database of server

3.2.5 S→B E(PU_b,K_s)||E(K_s,N_{ab})||E(K_s,M)

3.2.6 B: D(PR_b,K_s)→get K_s

D(K_s,N_{ab}) →get N_{ab}

D(K_s,M) →get M

SG(K_s,M)compare MS'=MS?

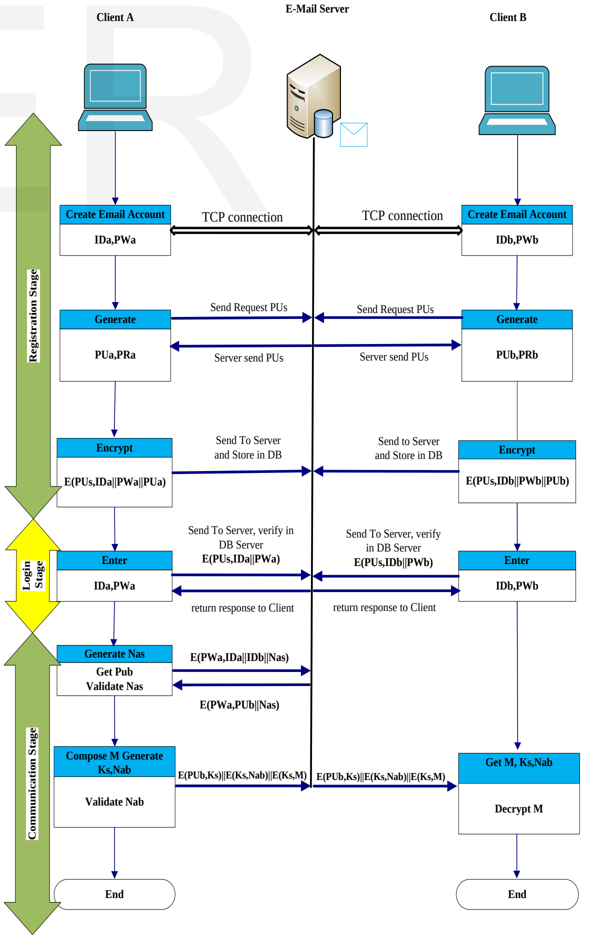
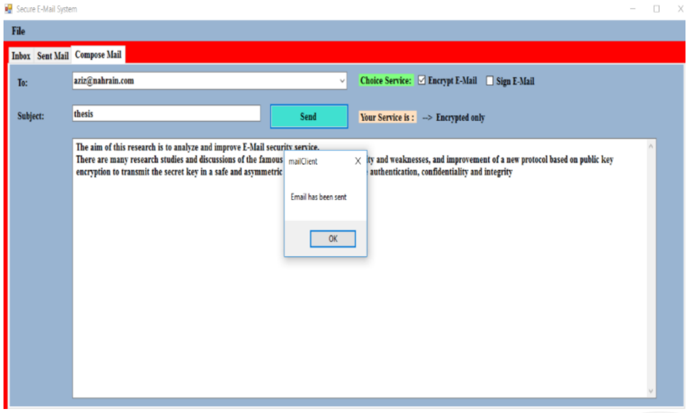


Fig. 2. Enhanced Proposed Secure E-Mail Protocol.

7 TEST OF THE SERVICES OF THE SYSTEM

7.1 Message Encryption Test

Fig. 3 illustrates an implementation test of the system, where user-A has composed a new message and send it with the encryption option to user–B. User-B has received the encrypted message and decrypts it to read it, as shown in Fig. 4. The encryption process is done by using AES 256 that make the encryption process secure enough to be broken by any hacker.



Secure E-Mail System

To: aziz@nahrain.com

Choice Service: ☑ Encrypt E-Mail □ Sign E-Mail

Subject: thesis

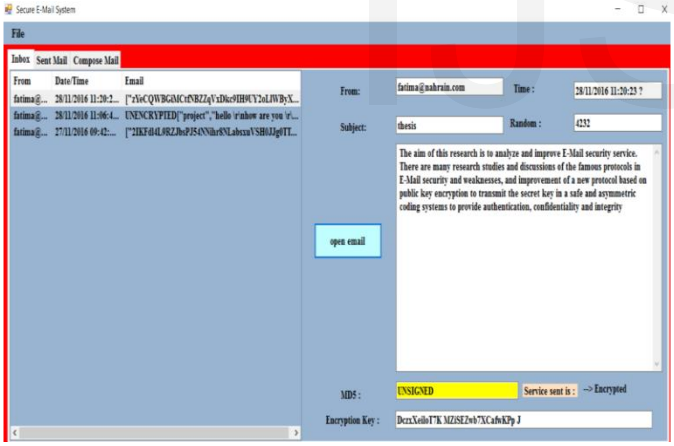
Your Service is : --> Encrypted only

The aim of this research is to analyze and improve E-Mail security service.
There are many research studies and discussions of the famous ty and weaknesses, and improvement of a new protocol based on public key encryption to transmit the secret key in a safe and asymmetric authentication, confidentiality and integrity

mailClient

Email has been sent

Fig. 3. Send Encrypted Message.



Secure E-Mail System

From	Date/Time	Email
fatima@...	28/11/2016 11:20:2...	["zYeCQWBGiMCtfNBZZqVxDkc9IH9UY2oLlWByX...
fatima@...	28/11/2016 11:06:4...	UNENCRYPTED["project","hello \r\nhow are you \r\...
fatima@...	27/11/2016 09:42:...	["2IKFdl4L9RZJbsPJ54NNihr8NLabsxuVSH0JJg0TT...

From: fatima@nahrain.com

Time : 28/11/2016 11:20:23 ?

Subject: thesis

Random : 4232

The aim of this research is to analyze and improve E-Mail security service.
There are many research studies and discussions of the famous protocols in E-Mail security and weaknesses, and improvement of a new protocol based on public key encryption to transmit the secret key in a safe and asymmetric coding systems to provide authentication, confidentiality and integrity

MD5 : UNSIGNED

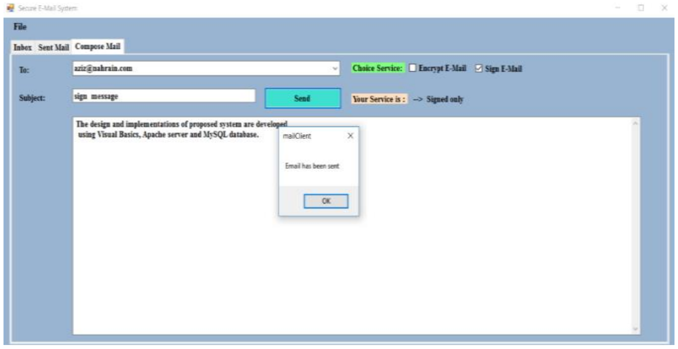
Service sent is : --> Encrypted

Encryption Key : DczxXeiloT7K MZiSEZwb7XCafwKPp J

Fig. 4. Received Encrypted Message.

7.2 Signed Message Test

In this option, we are testing the "Sign E-mail" option, where User-A composes and sends a message to User-B selecting "Sign E-mail" option, as shown in Fig. 5. When User-B receives the signed message and tries to open it and read it, the system would match the MD5 hash code of the received message with the MD5 of the sender (as shown in Fig. 6.), if they match, the system would open the message, otherwise the message is not allowed to be opened.



Secure E-Mail System

To: aziz@nahrain.com

Choice Service: □ Encrypt E-Mail ☑ Sign E-Mail

Subject: sign message

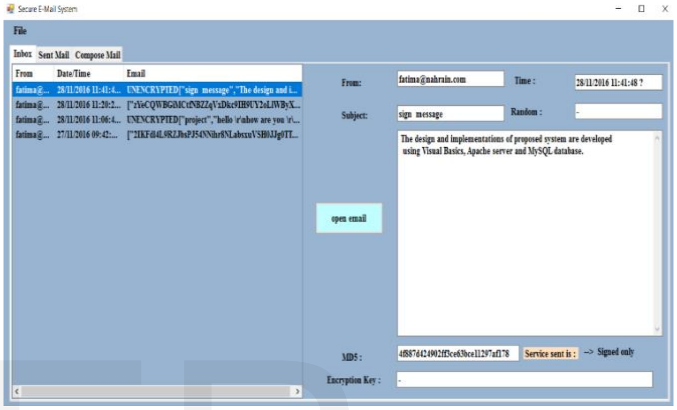
Your Service is : --> Signed only

The design and implementations of proposed system are developed
using Visual Basics, Apache server and MySQL database.

mailClient

Email has been sent

Fig. 5. Send Signed Message.



Secure E-Mail System

From	Date/Time	Email
fatima@...	28/11/2016 11:41:4...	UNENCRYPTED["sign message","The design and i...
fatima@...	28/11/2016 11:20:2...	["zYeCQWBGiMCtfNBZZqVxDkc9IH9UY2oLlWByX...
fatima@...	28/11/2016 11:06:4...	UNENCRYPTED["project","hello \r\nhow are you \r\...
fatima@...	27/11/2016 09:42:...	["2IKFdl4L9RZJbsPJ54NNihr8NLabsxuVSH0JJg0TT...

From: fatima@nahrain.com

Time : 28/11/2016 11:41:48 ?

Subject: sign message

Random : -

The design and implementations of proposed system are developed
using Visual Basics, Apache server and MySQL database.

MD5 : 4f887d424902ff3ce63bce11297af178

Service sent is : --> Signed only

Encryption Key : -

Fig. 6. Receive Signed Message.

8 CONCLUSIONS

The following conclusions were obtained from this work:

1. The proposed protocol manages the problem of the key ring management appeared in PGP system and resolves it by E-mail server key management system. In this system, the protocol is transparent to the user where only secret information is kept by the user with his password.
2. As many protocols are currently available for Email security such as SSL and TLS, it was proved that using a proposed protocol that can work sufficiently with the existing email application can also provide the desired security with less complexity.

9 REFERENCE

[1] Suresh Kumar Balakrishnan and V. P. Jagathy Raj, "Practical Implementation of a Secure Email System Using Certi_cateless Cryptography and Domain Name System", International Journal of Network Security, Vol.18, No.1, PP.99-107, Jan. 2016.

[2] Saritha P, Nitty Sarah Alex," Development of a Secure Mail Client", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 403-407.

IJSER

[3] Simon Josefsson, "Network Application Security Using the Domain Name System", Department of Numerical Analysis and Computer Science, Royal Institute of Technology SE-100 44 Stockholm, Sweden,2001.

[4] Mahmood Khalel Ibrahim, "Enhanced E-mail Security Protocol Based on Hybrid Cryptographic Systems", International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 5 Issue 3, March-2016.

[5] Mohammed Hassouna and et al, "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013.

[6] R. Sureswaran, Hussein Al Bazar, O. Abouabdalla, Ahmed M.Manasrah" Active E-mail System Protocols Monitoring Algorithm, University Sains Malaysia,2009.

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

[8] Arwa Husien, and Ghassan Samara, "Application Layer Protocols to Protect Electronic Mail from Security Threads", International Conference on Information Technology, ICIT 2015.

[9] Gori Mohamed.J, M. Mohammed Mohideen, Mrs.Shahira Banu. N" E-Mail Phishing –An open threat to everyone", International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.

[10] William Stallings," Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson, United States, 2009.

[11] Jim Kurose and Keith Ross," Computer Networking", sixth edition,2012.

[12] Sattarova Feruza Y. and Prof.Tao-hoon

[13] Kim," IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007.

[14] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy and A. Z. Ghalwash, "Chaotic Encryption Based PGP Protocol", International Journal of Computer Science and Telecommunications, Vol. 4, Issue 2, February 2013.

[15] Heinrich Moser," S/MIME", December 2001–January 2002.

[16] M. Tariq Bandai," Effectiveness and Limitations of E-Mail Security Protocols", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.3, May 2011.

[17] Shahin Fatima, Shish Ahmad, Shadab Siddiqui, "X. 509 and PGP Public Key Infrastructure methods: A critical review", IJCSNS International Journal of Computer Science and Network Security, Vol.15 No.5, May 2015.

[18] Atieh Saberi Pirouz," Securing Email Through Online Social Networks", Concordia Institute for Information Systems Engineering (CIISE), August 2013.

Author's Details:

Fatima Aziz and Mahmood Khalel Ibrahem
College of Information Engineering/ Department of Networks Engineering
Al-Nahrain University/ Baghdad-Iraq
mahmoodkhalel@coie.nahrain.edu.iq
ie_fatima@yahoo.com

IJSER