An End-to-End Secured Email System using Base64 Algorithm

Abolore Muhamin Logunleko
Department of Computer Science
Gateway ICT Polytechnic,
Saapade, Ogun State, Nigeria

Kolawole Bariu Logunleko
Dept. of Computer Science & Stas
DS Adegbenro ICT Polytechnic,
Eruku-Itori, Ogun state, Nigeria

Olanrewaju Olaide Lawal
Dept. of Computer Engineering
Moshood Abiola Polytechnic,
Abeokuta, Ogun State, Nigeria

ABSTRACT
In this present days, email system has turned out to be the broadly way to exchange information from one person to the other. Traditional email system is a one layer authentication system that is secured by username and password which are not enough to ascertain security. The email is connected through many routers and mail servers on its way to the recipient by becoming vulnerable to both physical as well as virtual eavesdropping by unauthorised person. This leaves a digital papers trail thereby more privacy and confidentiality of sensitive information is required. Encryption is of prime importance when confidential data is transmitted over the network. The system is developed to allow users to encrypt information before it is transmitted over the network. Base64 Algorithm was used for encryption and decryption of the information. This system runs on any device which works on windows operating system platform. The developed system secures the sensitive information sent through email by providing a secure, fast, and strong encryption which makes the mail very difficult for an attacker to interpret while in transmission thus making it resistant to forms of attacks. The various uses of this system in real life and its functionality are explained in this paper.

General Terms
Information Security, Encryption

Keywords
Base64 Algorithm, Decryption, Email, Encryption, Information

1. INTRODUCTION
Email has become a critical means in the modern competitive business. It is the backbone for most of the daily activities of business organizations and will continue to grow [2]. Many organizations deal with some forms of sensitive information which are often exchanged using e-mail. Therefore, e-mails security is vital in protecting the privacy of its users and their information from unauthorized viewing or alteration. Security is one important aspect of an information system. Any information sent is expected to be received only by those who have the right. Information can also be as useless as anything if at the time of transmission hijacked by an unauthorized person. That means that the network is prone to be intercepted. From time to time the data transmission technology has developed so rapidly. Security is highly necessary for an organization so as to maintain the integrity of the data and information. Security is becoming more and more essential as widespread and high speed networks are used to connect ever more devices together. In this networked world, the cost of intercepting and modifying data is much cheaper compare to the physical world. This is why such a variety of security tools need to be available for electronic mail communication. Electronic mail is used worldwide by linking through many routers and mail servers on its way to the recipient. This information can be become vulnerable to both physical as well as virtual eavesdropping by unauthorised person, which does not ensures four securities attributes, namely; availability, confidentiality, integrity and authenticity. In this paper, based64 algorithm model was developed to secure email communication system. The rest of the paper is arranged as follows: Section II provides existing literature and some related works. Section III focuses on the methodologies. Section IV presents the results and discussions and section V concludes the paper.

2. LITERATURE REVIEW
2.1 Conceptual review of Email
[4] reported that electronic mail or e-mail is a method by which a digital message is delivered from a sender to one or more recipients. [4][6] revealed that email is one of the fundamental internet technologies, a tool used by nearly every person with an internet connection. It allows you to, at no cost; send a letter of unlimited length to one person or many people at once, [10]. It arrives almost instantly, and they can reply straight away, [6].The history of electronic mail started at the Massachusetts Institute of Technology (MIT) in 1965 under the name Mailbox, with the aim of sending files from one computer to another. A major breakthrough was witnessed in the year 1971 with the appearance of a real email system, when Ray Tomilson who worked for the department of defence (DoD) sent his first ARPANET email message to himself [13].

2.2 Conceptual Review of Base64 Algorithm
[11] described Base64 algorithm as an algorithm that uses a concept of modern encryption algorithms. It is a block cipher algorithm that operates on a bit. Base64 algorithm encodes binary data and translates it into a representation of the base64. The term comes from the Base64 MIME (Multipurpose Internet Mail Extension) encoding specific content. [9] stated that base64 algorithm is often used when there is a need to encode binary data that needs to be stored and transferred through media designed in form of textual data. This is to make sure that the data strictly remains intact without modification during shipping. Therefore, Base64 can be used in different applications such as email through MIME and storage of complex data in XML. Hence, Base64 needs to be learned because the transformation of base64 is widely used on the Internet as a medium to transmit data format. Due to the result of the transformation of base64 to plain text, and then this value will be much more easily shipped, compared to the form of binary data format.

2.3 Review of Related Works

Shreenath et. al. (2014) [2] developed a system that helps to secure the sensitive information sent through email by providing a three layer authentication mechanism.

Suresh et. al.(2012) [3] presented email system based on IBE which makes use of DNS as the setup for key exchange, a proxy service that carry out encryption and decryption in the best interests of user and a secure key token for user authentication.

Guwalani et. al. (2014) [9] did a research on Image File Security using Base-64 Algorithm. The paper mainly focused on embedding the data from one format to another by designing a data conversion application which converts image file to text file and text file to image file. Usually, image loses its resolution after conversion of image is done. The authors proposed a method such that the image remains unchanged in its resolution as well in size.

Martin et. al. (2002) [12] designed a new protocol relying on a light on-line trusted third party. It aimed at combining security, scalability, easier implementation and viable deployment. Its implementation does not require any special software at the receiver as well as no need of on-line servers at the sender. It specifically utilizes a Java enabled browser with SSL and supports several methods of practical authentication without relying on public key infrastructure making it suitable security measure for existing web and email infrastructure.

Mohammed et. al. (2013) [13] conducted a research on a mailing system that is based on certificateless cryptography. In the proposed mailing system, the message payload is encrypted by a per-mail symmetric key generated from a secret value, the public and private keys of the sender and the receiver at each side. The developed mailing system is secured against standard security model and provides many security properties.

Abadi et. al. (2003) [1] designed a protocol for certified e-mail delivery that appears to have many practical advantages. Although it requires a trusted third party (TTP), this TTP is stateless and lightweight; it never has access to the clear-text of the transmitted messages. The burden on the TTP is independent of the message size. No public-key infrastructure is necessary. The TTP must have signature and encryption keys, but other principles merely share a secret with the TTP, such as a password.

Ada et. al. (2017) [5] designed and prototyped Confidante, an encrypted email client that uses Key based for automatic key management thereby conduct a user study with 15 people (8 U.S. lawyers and 7 U.S. journalists) to evaluate Confidante's design decisions and find that users complete an encrypted email task more quickly and with fewer errors using Confidante than with an existing email encryption tool, and that many users report finding Confidante comparable to using ordinary email. However, the paper also finds that lawyers and journalists have diverse operational constraints and threat models, and thus that there may not be a one-size-fits-all solution to usable encrypted email.

3. METHODLOGY

3.1 Algorithm

3.1.1 Base64 Algorithm Encryption Procedures (B64)

Procedures for Base64 Encryption process is explained below:

1. Provide the Plain Text
2. Get the ASCII Number of Each Text.
3. Convert Each ASCII Number to 8 bits Binary Number
4. Merge the 8 bits Binary Number to form 24 bits Binary Number.
5. Split the 24 bits Binary Number to 6 bits Binary Number Each.
6. Convert Each 6 bits Binary Number into Decimal Number Equivalent.
7. Finally, Use the Decimal Number to get its Equivalent from Base64 Characters Table which formed the Encrypted Text.

3.1.2 Base64 Algorithm Decryption Procedures (B64)

Procedures for Base64 decryption process is explained below:

1. Provide the Encrypted Text
2. Get the Decimal Number Equivalent of Each Encrypted Text from Base64 Characters
3. Convert Each Decimal Number Equivalent into 6 bits Binary Number.
4. Merge Each 6 bits Binary Number to form 24 bits Binary Number.
5. Split the 24 bits Binary Number to form 8 bits Binary Number Each
6. Convert each 8 bits Binary Number into Decimal Number.
7. Finally, Use the Decimal Number to get its Equivalent from the ASCII Code Table which formed the Plain text.

3.2 Base64 Encryption and Decryption Algorithm Flow Charts

Figure 1 and Figure 2 show the flow chart for the encryption and decryption algorithm respectively.

3.3 System Architecture

Figure 3 is the proposed system architecture. The basic operation in this regard is for the sender to log in into the system, select encryption, fill the information and send it. On the receiving end, the receiver log in and select decryption, paste the information and view it.

4. RESULTS AND DISCUSSIONS

The developed system is an email client that uses java programming language for implementation and Base64 algorithmic model was integrated into the electronic mail system. The developed system was tested on this system configuration:

Manufacturer: Samsung Electronics

Rating: 2.3 Windows Experience Index

Processor: Intel(R) Atom(TM) CPU N2100 @ 1.60GHz 1.60 GHz.

Installed Memory: 4.00GB (3.24 GB Usable)

System Type: 64-bit Operating System

The plaintext are encrypted over this secured electronic mail communication system at a very fast speed through the sender and then decrypted in the same manner by the receiver. In addition, the developed system is suitable and easy to

implement on a system for use. Series of tests were performed on encryption and decryption. The result shows that the system performed very well on the computer and there are no negative effects on the computer performance. The computer performance of the developed system showed that the developed system is a secured mail client which makes it the best alternatives for securing electronic mail. Moreover, the proposed system does not slow the performance of the computer.

Above all, sequences of random messages called plaintext were used to test the developed system on the different computers to impose security on plaintext in other to ensure the confidentiality and the integrity as shown in figure 4, 5 and 6 respectively.

4.1 Comparison

A comparative study between the Traditional Email System, TES and the Proposed Email System, PES is presented in the Table 1 utilizing eight factors which are Encryption, Decryption, Power Consumption, Speed, Layer of Security, Security, Internet and Hardware and Software Implementation.

5. FIGURES/CAPTIONS

Table 1: Comparison between TES and PES

Factors	**TES**	**PES**
Encryption	Not Applicable	Applicable and Fast
Decryption	Not Applicable	Applicable and Fast
Power Consumption	Low	Low
Speed	Faster	Fast because of decryption process
Layer of Security	One	More
Security	Not Secure Enough	Highly and Adequately Secure
Internet	Required	Required for encryption but may and may not require for decryption
Hardware and Software Implementation	Better in Software but not efficient in hardware	Better in Software but not efficient in hardware

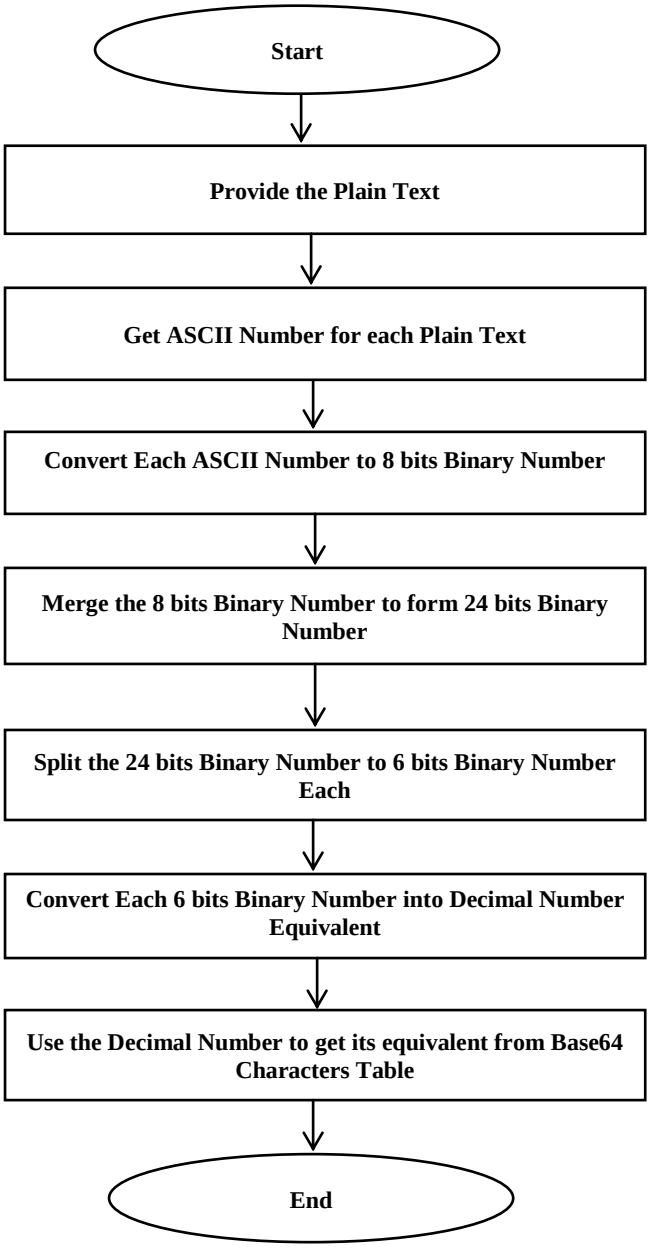

Figure1: Base64 Encryption Flow Chart

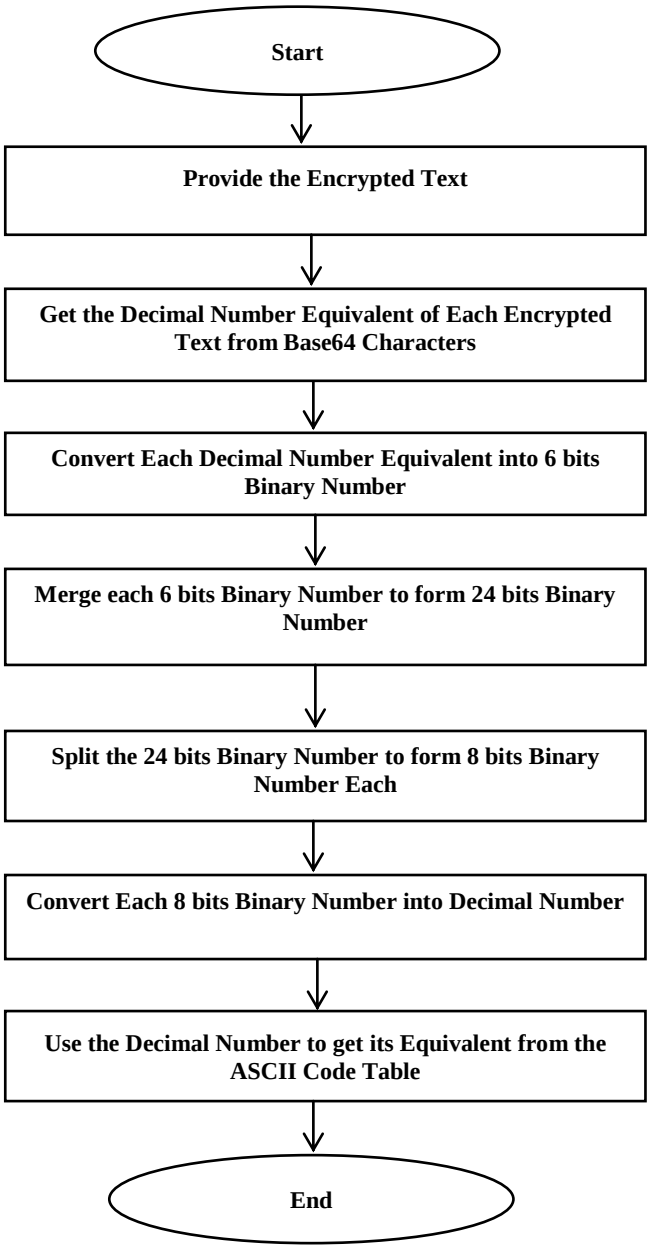

Figure2: Base64 Decryption Flow Chart

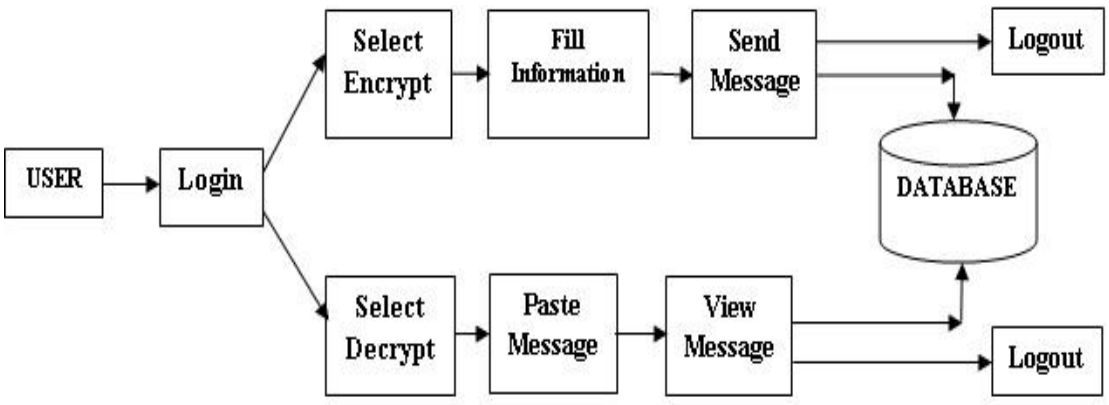

Figure 3: The Proposed System Architecture

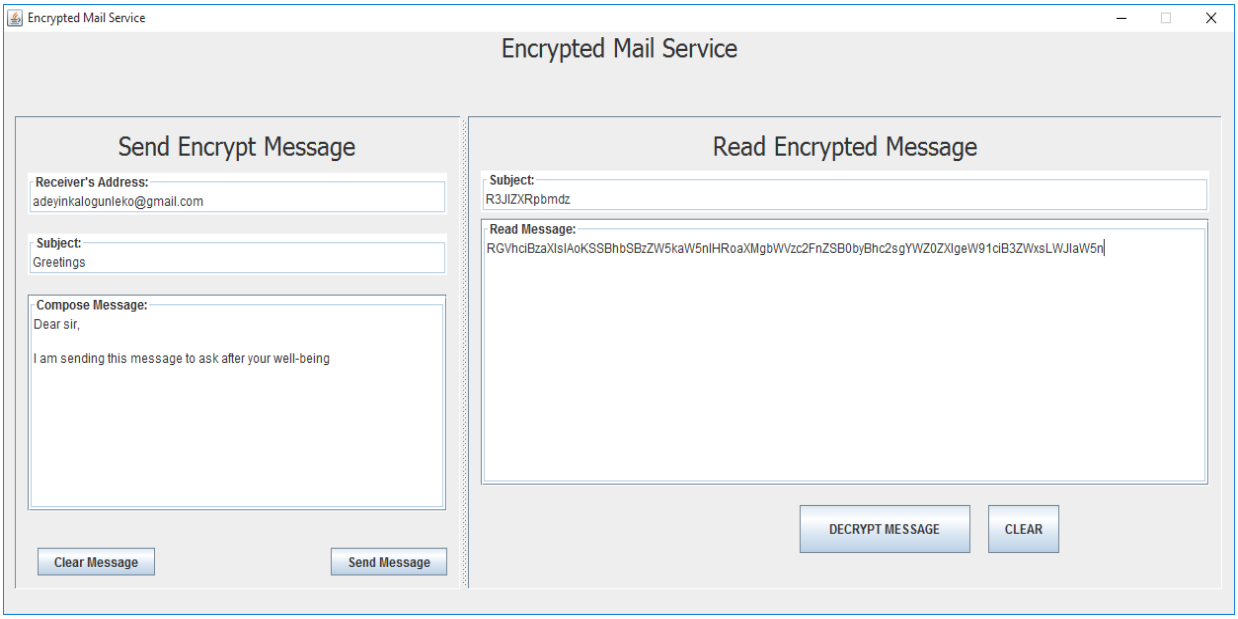

Figure 4: Encrypted Message Page

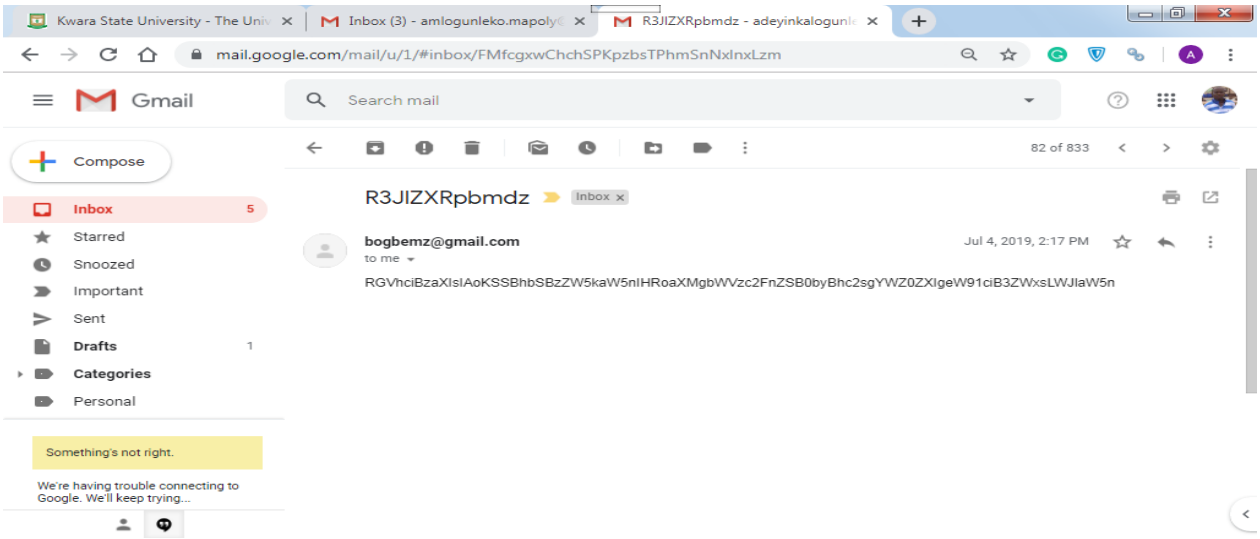

Figure 5: Inbox Page

Figure 6: Decrypted Message Page

6. CONCLUSION

The paper presented an end-to-end secure email system using base64 algorithm. The user experiences no delays while using the system, which is a clear indication that the speed requirement is met. The system user interface is simple and straight forward to use. The system provides online service, doing email encryption and decryption on behalf of registered users. The approach is that all existing email functionality is preserved and significant new infrastructure is added, which made the scheme to significantly reduce phishing and potentially mitigate spam. The solution depends on the base64 algorithm as a secure component of a cryptographic architecture. So, the base64 algorithm comes under more scrutiny. There is a need to further secure base64 algorithm and generally establish a highly secure mechanism for distributing certified domain specific information.

7. REFERENCES

[1] Abadi, M., and Blanchet, B. (2003).Computer-Assisted Verification of a Protocol for Certified Email, Static Imperial College Press 200,ISBN 978-1-86094-866-4.

[2] Shreenath, A., Aureen, G., Deepthi, S and Tania, P., (2014) "Smart Mailing System for Secure Transmissions" *International Journal of Computer Applications* Pp0975 – 8887, Volume 96– No.22.

[3] Suresh, K. B. and Jagathy, R. V.(2012): 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, ISSN 2079-8407.

[4] Tech Savvy Senior (2018). Introduction to email part1, Beginner guide.

[5] Ada, L., Eric, Z., and Franziska, R. (2017).Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists, IEEE European Symposium on Security & Privacy.

[6] Burke County Public Library (2010). Electronic Mail Basics. Retrieved from www.bcpls.org

[7] Christa, D. and Carmen, F. (2016): Email Communication Pp35-54. Retrieved from https://www.researchgate.net/publication/280703829

[8] Giampaolo, B., Cristiano, L., and Lawrence, C. (2003).Verifying Second-Level Security Protocols, Lecture Notes in Computer Science, Volume 2758, pp 352-366, Springer Berlin Heidelberg.

[9] Guwalani P, Kala M, Chandrashekar R, Shinde dan J and Mane D. (2014). Image File Security using Base64 Algorithm, *Int. J. Computer Technology & Applications*, vol. 5, no. 6, pp. 1892-189.

[10] Karen, R., Judith, R., and Mario, H.(2006). You've Got E-Mail!… Shall I Deal With It Now? Electronic Mail from the Recipient's Perspective, *International Journal of Human Computer Interaction*, 21(3), 313–332.

[11] Logunleko K. B, Logunleko A. M, Akinwunmi O. O. & Lawal O. O. (2019): Security Assurance Framework for Intelligible Information Using a Customized Base64 Encryption Algorithm *Proceedings of the 17th iSTEAMS Multidisciplinary Research Nexus Conference*, D.S. Adegbenro ICT Polytechnic, Itori- Ewekoro, Ogun State, Nigeria, 21st – 23rd July, 2019.Pp 85-93 . www.isteams.net - DOI Affix - https://doi.org/ 10.22624/AIMS/iSTEAMS-2019/V17N2P10

[12] Martin, A., Neal, G., Bill, H., and Benny, P.,(2002) "Certified email with a light on-line trusted third party: Design and implementation", *11th international conference on world wide web*, pp. 387- 395, ACM, New York, ISBN:1-58113-449-5.

[13] Mohammed, H., Nashwa, M., Bazara, B., and Eihab, B.,(2013) "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model" in *IJCSI International Journal of Computer Science Issues*, Vol. 10, Issue 2, No 3,Pp 264-271,ISSN (Print): 1694-0814| ISSN (Online): 1694-0784

[14] Robbi, R. (2018). Combination Base64 Algorithm and EOF Technique for Steganography. *International Conference on Information and Communication Technology (IconICT): Journal of Physics*: Conf. Series 1007.