International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 10, October - 2013

Achieving Non Repudiation Services With Certified Email Delivery System

S Jeelan

Associate Professor,
Department of Computer Science & Engineering,
S.V.P.C.E.T., Puttur.

E Ugandhar

PG Scholar,
Department of Computer Science & Engineering,
S.V.P.C.E.T., Puttur.

Abstract

Even though email is an increasingly important application, the Internet doesn't yet provide a reliable messaging infrastructure. Thus, an email message's sender can never be certain- and doesn't receive any evidence- that his or her message was actually delivered to and received by its intended recipients. Furthermore, a recipient can always deny having received a particular message, and the sender can't do much to prove the opposite. This lack of evidence for message delivery and reception is actually a missing piece in the infrastructure required for the more widespread and professional use of email.

Against this background, my current project address problem of providing certified mail services. In certified mail services sender gets a delivery report for the corresponding mail. Certified mail provides proof of delivery and dispute resolution in many cases. In this system Trusted Third Party (TTP) acts an intermediary between sender and receiver.

1. Introduction.

In current days Internet plays a vital role in communication. In that email services occupied peak position. Emails are widely using for offline messages. Many software corporations in the Internet provide email services for free of cost. Some of the famous email service providers are Yahoo, Gmail, and Hotmail.

In the current form, the Internet doesn't provide a reliable messaging infrastructure. Steps in present system mail delivery are

- Compose mail
- Sent to the receiver

The several missing pieces that existing in the current form of mail infrastructure are

- Acknowledgement of delivery
- Evidence of delivery to the intended receiver
- Denying of receive message
- No provision of non-repudiation services

This lack of evidence for message delivery and reception is actually a missing piece in the infrastructure required for the more widespread and professional use of email.

Against this background, my current project address problem of providing certified mail services. These certified services lead to dispute resolution.

Email services are prominent in the services provided by the Internet. Even though email is an increasingly important application, the Internet doesn't yet provide a reliable messaging infrastructure.

Present email service infrastructure, an email message's sender can never be certain- and doesn't receive any evidence- that his or her message was actually delivered to and received by its intended recipients. Furthermore, a recipient can always deny having received a particular message, and the sender can't do much to prove the opposite. This lack of evidence for message delivery and reception is actually a missing piece in the infrastructure required for the more widespread and professional use of email.

In certified mail services sender gets a delivery report for the corresponding mail. Certified mail provides proof of delivery and dispute resolution in many cases.

Main objective of providing certified mail service is to provide the delivery report for respective sender of corresponding mail. Along with this some other objectives are

- Proof of delivery to intended receiver
- Dispute resolution
- To improve professional usage of mail services

2. Existing System.

Present email service infrastructure, an email message's sender can never be certain- and doesn't receive any evidence- that his or her message was actually delivered to and received by its intended recipients. Furthermore, a recipient can always deny having received a particular message, and the sender can't do much to prove the opposite.

With existing system following are some of the problems

I. No Acknowledgement of delivery
II. No Evidence of delivery to the intended receiver
III. Denying of receive message
IV. No provision of non-repudiation services

This lack of evidence for message delivery and reception is actually a missing piece in the infrastructure required for the more widespread and professional use of email.

3. Proposed system.

In proposed system i.e., in the certified mail services [1] there will be acknowledgement or proof of delivery for the sender's mail. These acknowledgement or proof of delivery act as an evidence for the sender. In this system Trusted Third Party (TTP) acts an intermediary between sender and receiver. TTP also acts an server in the actual implementation.

4. Objective and Architecture.

Following architecture gives outline of working certified mail services on the Internet using TTP Web server. Architecture contains sender, receiver, TTP Web server and messages among them.

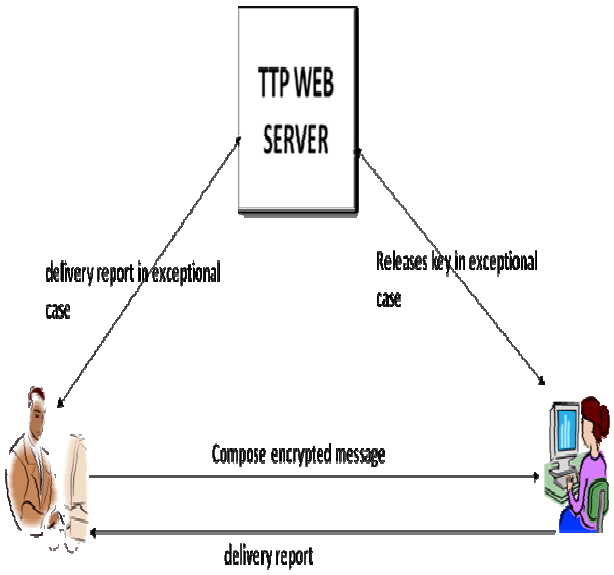

Figure 1. Architecture of Offline TTP

5. Problem Solution.

5.1 Symmetric Key Encryption.

Symmetric key encryption uses same key, called secret key, for both encryption and decryption. Users exchanging data keep this key to themselves. Message encrypted with a secret key can be decrypted only with the same secret key. The algorithm used for symmetric key encryption is called secret-key algorithm. Since secret-key algorithms are mostly used for encrypting the content of the message they are also called content-encryption algorithms.

5.2 Asymmetric Key Encryption.

Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made public called public-key. Hence this is also called Public Key Encryption [2]. A private key is typically used for encrypting the message-digest; in such an application private-key algorithm is called message-digest encryption algorithm. A public key is typically used for encrypting the secret-key; in such an application private-key algorithm is called key encryption algorithm.

Popular private-key algorithms are RSA and DSA (Digital Signature Algorithm). While for an ordinary use of RSA, a key size of 768 can be used, but for corporate use a key size of 1024 and for extremely valuable information a key size of 2048 should be used.

Non-repudiation services must ensure that when sender does not send some information to recipient over a network, sender nor recipient can deny having participated in a part or the whole of this communication. Therefore a fair non-repudiation protocol has to generate non-repudiation of origin evidences intended to recipient, and non-repudiation of receipt evidences destined to sender. In this paper, we clearly explained important of non-repudiation protocols with trusted third party (TTP).

TTP is a security authority that performs security related functions and cryptography methods [3]. Various types of TTP can be considered according to their involvement in the protocol.

This paper presents providing a certified and non-repudiation email services on internet. The project aims to combine security, return receipt or report of delivered mail, easy implementation, and viable deployment. In general, the main goal is to guarantee that the receipt of an email message produces a receipt certificate to the sender. Secondary goals such as authenticity of sender and receiver and message confidentiality.

To implement proposed system many technologies are available like Online TTP, Offline TTP, Inline TTP and No TTP. Among these Offline TTP is advantageous because TTP is invoked only in the exceptional cases. Functioning of Offline TTP is as follows

1. The user composes and sends a Certified Mail message [4] (message with key) from their email client or web browser.
2. The email is transmitted to receiver, if the receiver clicks that message then delivery report is reached to sender. But the key is required to open that message.
3. Whenever the delivery report is reached the sender then sender has to send the key to receiver to open message.
4. If the two parties have done any mistake between their interactions then offline TTP exists that means if problem exists for sender then interactions between sender and TTP exists. Similarly for the receiver.

6. Future Work.

To provide a reliable service with TTP services can be done in an efficient way, to do so that implementation has to be programmed use in mobiles. This mean if a sender sending an email to a person, that when recipient retrieve all the mails in different time, at this time the sender may not available online, in this case a delivery notification can be send the sender's mobile device that the particular recipient has received your mail at this time [5]. By enabling this can be useful to the users who use emails for a particular time.

Another improvement, when a sender sending a mail all sent items will be saved in his/her sent items folder. Once the recipient has retrieved the mails that sent mail in the sent item folder will change into a different color and it contains the details such as Date and time and IP address of the recipient. This also a useful method of providing certified mail services over the Internet.

7. Conclusion.

This system can provide a certified mail service on the internet using Trusted Third Party. A sender can assure that his/her mail has reached to the correct destination. This will give the details such as when the recipient retrieved the messages from the mail server and which IP Address he/she used to retrieve the messages. This can be more useful to people who send business purpose which needs a delivery report.

TTP server has to check all outgoing mails and it has to get all the details of recipient, in real time this cause major delay to deliver the mails on time. This may be a main drawback of this system. When getting all the details of the client by TTP can be cause for huge network traffic, this is also a drawback from this system. It is no need for both parties to have this Certified Mail to get reliable service. Sender having this Certified Mail is enough to get the delivery report.

8. References.

[1] R. Oppliger, "Certified Mail: The Next Challenge for Secure Messaging," *Comm. ACM*, vol. 47, no. 8, 2004, pp. 75–79.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM*, vol. 21, no. 2, 1978, pp. 120–126.

[3] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm," *IEEE Trans. Information Theory*, IT-31, no. 4, 1985, pp. 469–472.

[4] A. Bahreman and J.D. Tygar, "Certified Electronic Mail," *Proc. Internet Society Symposium on Network and Distributed System Security*, IEEE CS Press, 1994, pp. 3–19.

[5] T. Coffey and P. Saidha, "Nonrepudiation with Mandatory Proof of Receipt," *ACM SIGCOMM Computer Comm. Rev.*, vol. 26, no. 1, 1996, pp. 6–17.