Smart Mailing System for Secure Transmissions

Shreenath Acharya
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Aureen Gomes
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Deepthi Suvarna
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Tania Paulson
Dept of ISE
St. Joseph Engineering College
Mangalore, India

Vishrutha
Dept of ISE
St. Joseph Engineering College
Mangalore, India

ABSTRACT

Email system has become the widely preferred means of information transfer in the modern business. Conventional email system is secured by a password system leading to a single layer of protection which is insufficient for guaranteed security. Modern businesses are more relying on electronic mail for communication with their clients and colleagues revealing the need for more privacy of sensitive information. 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. The current industry standards do not place much emphasis on security as the information is transferred in plain text and the mail servers will be regularly performing the backups of the emails passing through. This leaves a digital paper trail that can be easily inspected months or years later which can be read by any cracker who gains access to an unprotected router. The proposed system helps to secure the sensitive information sent through email by providing a three layer authentication mechanism.

Keywords

One Time Password (OTP), Email, Encryption, Decryption, Authentication, Plain Text, Cipher Text

1. INTRODUCTION

Email has become a critical means in the modern competitive business. It is the backbone [1] for most of the daily activities of business organizations and will continue to grow. A larger risk to email data within the enterprise is illegitimate access to sensitive information from the mailbox. It may be through the links or from the administrator resetting knowing the higher officials password. Thus, authentication and security of mailbox data are the essential factors to be closely monitored in order to ensure that the email system data is available to only legitimate users. The increased usability of the email access via the Internet poses another security threat for business mail systems from the email clients illegally accessing the critical information. It calls for special attention towards investing in mechanisms to control illegal access to email data via the Internet. Thus, creating a secure environment that could be proactively and efficiently managed requires a comprehensive solution involving third party add-ons to address all the security issues in business.

The critical information sent through the email can be considered secure by making sure the facts like [2]: convincing the receiver that message is from intended sender, it could be read by only the intended recipient and there is no chance that someone could have tampered the content during its transmission. The use of secure Internet protocols like secure IMAP and secure POP [3] enhance content secrecy by encrypting the content of an e-mail transparently before they are transmitted from a mail server to a user over the Internet.

The proposed system intends to develop an email server which could be used for secure transmission of information in any organization by way of three layer authentication technique. It provides a user friendly interface characterized with the three main essentialities of the ideal mailing system. ie, simple, safe and secure. The main objective is to provide a reliable environment for users to communicate the confidential informations related to their specific needs in their organizations.

The remainder of the paper is organized as follow: Section II describes the literature survey. Section III depicts the architecture of the system. Section IV contains the algorithmic & flow chart representation of the implementation. Section V discusses the result and the analysis of the system’s performance. Section VI concludes the paper.

2. LITERATURE SURVEY

According to the Radicati Group’s study, “Microsoft Exchange and Outlook Analysis, 2005-2009,”[4] the worldwide email market will grow from 1.5 billion mailboxes in 2011 to 2.8 billion mailboxes in 2012. Managing large, active stores of information takes time and effort in order to avoid failures – failures that will impact the users and therefore the business, undoubtedly leading to lost productivity. For secure and effective storage management, organizations must take a proactive approach and invest wisely in a comprehensive solution.

Giampaolo Bella et al. [5] proposed a system by developing the concept of a second-level security protocol that uses a first-level protocol as a primitive, showing how correctness assertions for second-level protocols can be expressed. The existing primitives of the Inductive Approach already lets it formalise such concepts as sending a confidential message, an authenticated message, or a message with guaranteed delivery.

Dan Zhou et al. [6] describe the application of their development process to the development of a Privacy Enhanced Mail (PEM) system. The purpose of this work was to demonstrate an integrated verification and synthesis process on an engineering application. Higher-order logic bridges the two systems used for verification and for synthesis; it is a useful intermediate language for relating formal tools. The automatically generated code was not as concise as custom designed code. Nevertheless, it was assured code that worked. In constructing this system, we developed an algebraic specification for each component of PEM. The use of abstract data type helps partition the system into modules, which should increase system maintainability. The emphasis on modularity and composition has been beneficial. Rebuilding the system became easier when components were changed.

M. Abadi et al. [7] have 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.

The cryptographic protocols are made more secured by using inductive definitions [8] based on ordinary predicate calculus and copes with infinite-state systems. It uses Isabelle/HOL (Higher Order Logic) for generating proofs. Here the protocols are inductively defined as set of traces. A trace is a list of communication events comprising many interleaved protocol runs. Protocol descriptions incorporate attacks and accidental losses and the model spy knowing some private keys can forge messages using components decrypted from previous traffic. The three protocols analyzed are Otway-Rees (uses shared-key encryption), Needham-Schroeder (uses public-key encryption), and a recursive protocol (variable length).

Martin Abadi et al. [9] 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.

Brian Donadi [10] states that E-Mail services must be able to provide Non-Repudiation and Encryption when necessary. A secure E-Mail system or client also must be able to minimize the effects of spam and malware on the systems that receive messages. E-Mail processes need to be reviewed and updated as newer protocols and technologies are developed. The most successful E-Mail systems use the best options together to allow users to access E-Mail the easiest and most secure way possible.

The application of inductive methods to Transport Layer Security (TLS) [11] is more complicated than other existing protocols since the session keys are negotiated rather than being distributed. The inductive method translates each protocol step into a rule of inductive definition which is 15 for TLS. Here, the parties have a secure channel once the session keys have been established. But, the authors assumed that application data does not contain secrets associated with TLS sessions such as keys and master secrets. If it does, one security breach could lead to many errors.

3. PROPOSED SYSTEM ARCHITECTURE

The architectural diagram of the proposed system is shown in figure 1. It clearly depicts the working of the system.

A user must first create an account to avail the services provided by the developed mail system and the details are saved into the database. While signing up, it is necessary to enter the valid secondary email id and mobile number he is using presently. Then the user logs in providing a valid user name and password which provides the first level of security. After logging in, the user can check his mails in inbox, compose mails, check sent items and can manage his contacts. While composing mails, the user can send a normal message or a critical message. The normal mail can be sent by selecting the normal button to the mail id of the receiver. On selecting the secure button, the critical messages can be sent to the appropriate receiver.

At the sender's side, the mail is first encrypted and then divided into two parts non sequentially. One part goes to developed mail system while the other part is sent to the secondary mail id provided by the user during the registration procedure. An OTP is generated and sent through sms gateway. On receiving the normal message, the receiver can read the message directly by clicking the view button in his inbox. On receiving a secure mail, the user has to click on the view button which then goes to the merge page where part 1 message, received through the proposed mail system id, can be automatically seen in the merge page and part 2 message received in the user's secondary mail id should be manually downloaded. This text file will be saved in a drive in the system which then has to be browsed in the merge page. The text file which is downloaded will have the name of the subject appended with extention .txt indicating that it is a text file. Afterwords the OTP received on the registered number within the sign up page is entered to retrieve and view the original message. The receiver need to make sure the file that is browsed and the OTP entered is correct and valid. The Encryption, Decryption, Divide and Merge processes provide the second level of security while the OTP generation is the third level of security.

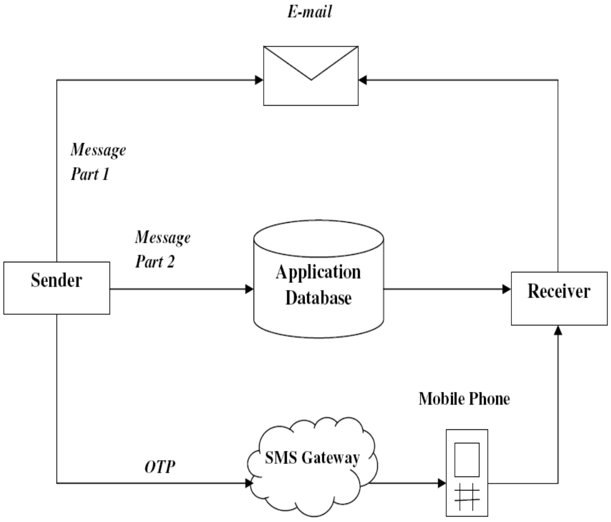


Figure 1. Architectural Diagram

4. ALGORITHM AND FLOW DIAGRAM

4.1 Algorithm for Compose Mail

```
If (Secure is selected)
        Then
                Encrypt the message
                Divide Non Sequentially
                Generate OTP
                Send Secure message in two parts
        Else
```

```
                Normal message is sent
Endif
```

4.2 Algorithm for Receive Message

```
If (Secure message received)
        Then
                Receive part 1 from existing mail
                Retrieve the part 2 from the application
                Input Received OTP to merge, decrypt and
                read the original message
        Else
                Read Normal message from Mystery Mail
Endif
```

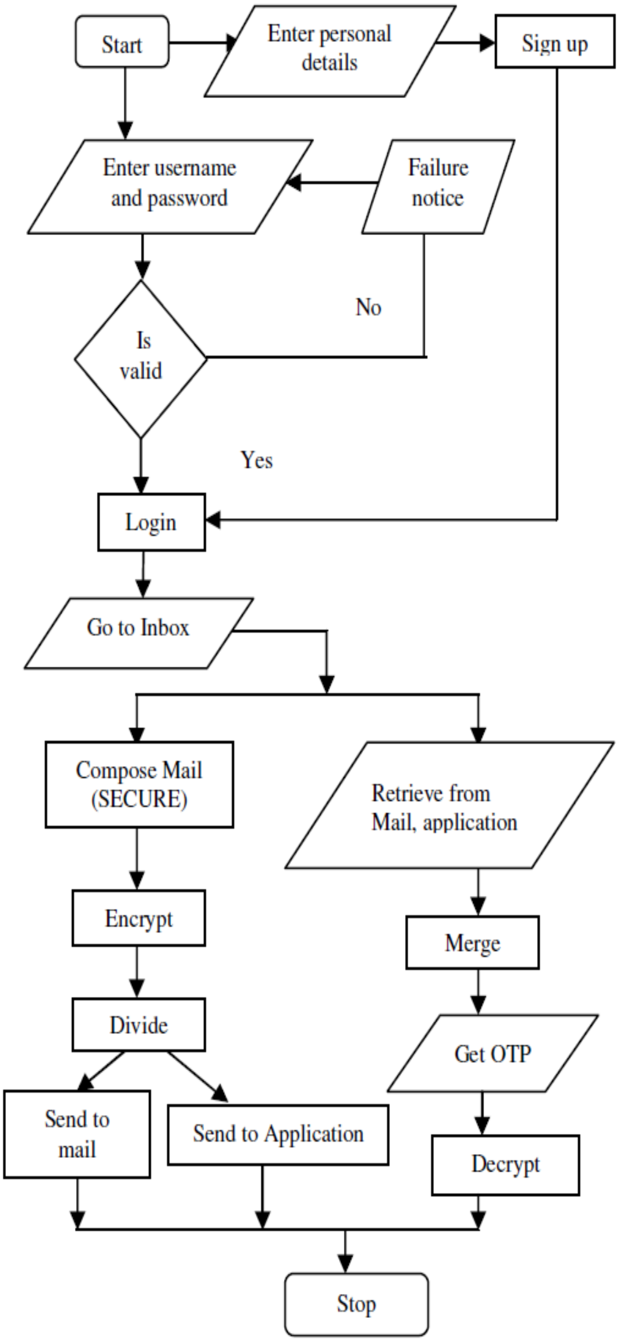
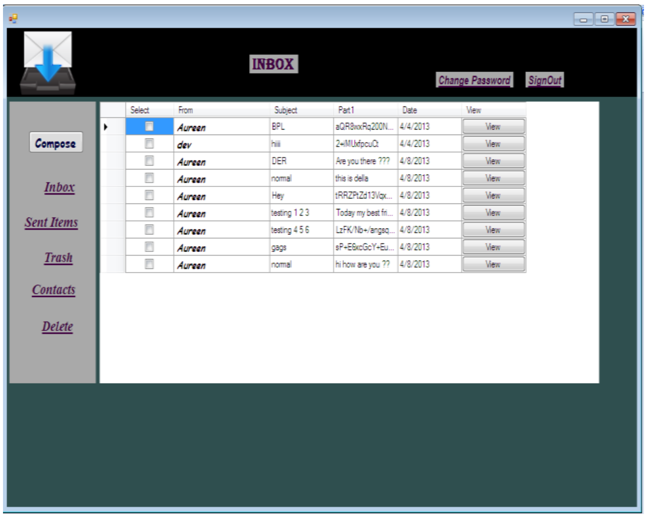


Figure 2. Flow diagram

Figure 2 shows a flowchart describing the sequence of steps for sending and receiving of critical mails via the Internet.

5. RESULTS

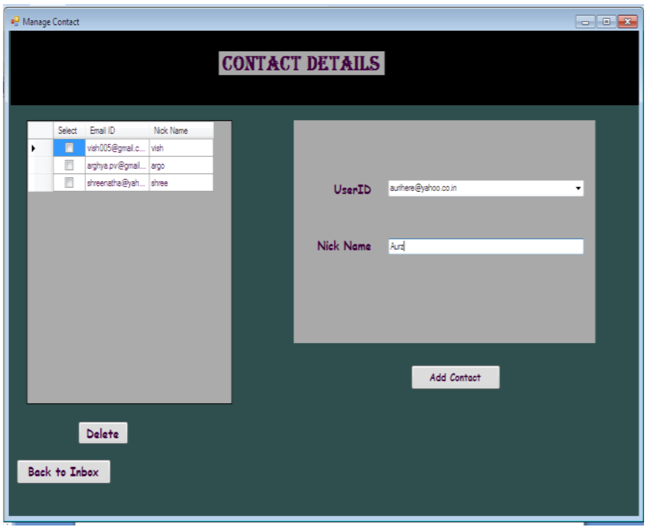
The implementation of the algorithm has been carried out in the dot net IDE using C sharp as the programming language. The Advanced Encryption Standard (AES) ie, Rijndael algorithm is utilized for performing encryption and decryption.



	Select	From	Subject	Part1	Date	View
▸	□	Aureen	BPL	aQR8wxRq200N...	4/4/2013	View
	□	dev	hiii	2+iMUxfpcuCt	4/4/2013	View
	□	Aureen	DER	Are you there ???	4/8/2013	View
	□	Aureen	normal	this is della	4/8/2013	View
	□	Aureen	Hey	tRRZPtZd13Vqx...	4/8/2013	View
	□	Aureen	testing 1 2 3	Today my best fri...	4/8/2013	View
	□	Aureen	testing 4 5 6	LzFK/Nb+/angsq...	4/8/2013	View
	□	Aureen	gags	sP+E6xcGcY+Eu...	4/8/2013	View
	□	Aureen	normal	hi how are you ??	4/8/2013	View

Figure 3. Inbox

The Inbox has different forms like the Inbox, Sent Items, Trash, Contacts, Delete labels and Compose links which will redirect to the respective forms based upon the respective selections.



	Select	Email ID	Nick Name
▸	□	vish005@gmail.c...	vish
	□	arghya.pv@gmail...	argo
	□	shreenatha@yah...	shree

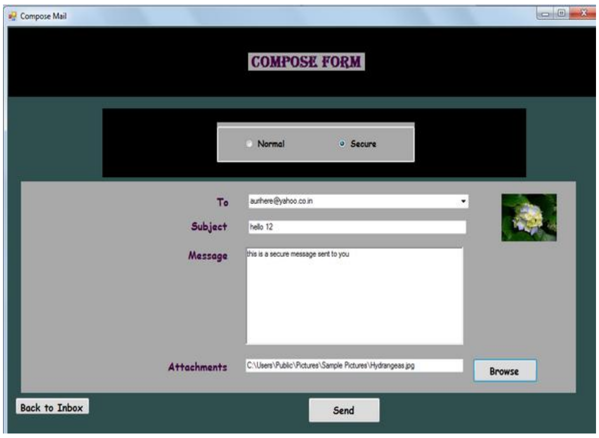
UserID: aurhere@yahoo.co.in

Nick Name: Aura

Figure 4. Managing Contacts

The contact details of all the users will be displayed by manage contacts for possible selection of recipient(s) to send message(s). It also provides provision for deleting the unwanted contacts from the system.

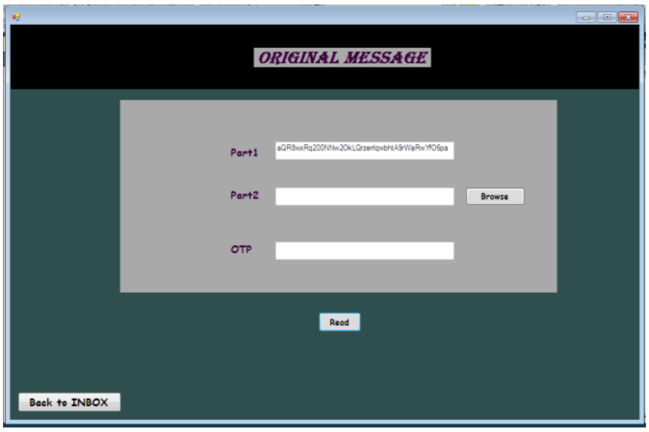
The Compose page provides a user with option to Mail. The user can send a normal or a secure mail. If he selects normal mail, the message will be sent to the corresponding recipient like traditional mail servers with lesser security. If the secure message format is selected, the message to be sent is encrypted and split into two parts. The one part goes to registered mail id of the proposed system and the other part goes to the existing mail id of the receiver.



To: aurhere@yahoo.co.in
Subject: hello 12
Message: this is a secure message sent to you
Attachments: C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg

Figure 5. Composing Secure Message

The figure 6 describes the merging of the two parts at the receiver to see the original message. It is carried out by browsing the part2 and entering the received OTP.



Part1: aQR8wxRq200NNw2OkLQrzerlqwbhtA9rWaRwYfO6pa

Figure 6. Merging two parts of Secure Message

Table 1 shows the comparison of the proposed mail system with the existing mail servers based on some specific parameters.

Table 1: Performance comparison with the existing system

Parameter	Existing Mail System	Mystery Mail (Normal Mail)	Mystery Mail (Secure Mail)
Integrity	Moderate	Moderate	High
Security	Low	Low	High
Authenticity	Moderate	High	High
Availability	Moderate	High	Moderate
Confidentiality	Moderate	Moderate	High
Overall Performance	Moderate	High	Moderate

As described in table 1, Integrity is relatively higher in the proposed system than in the existing systems because of the inclusion of the concept of sender receiving an acknowledgement from the receiver once he reads the original message. This feature is not present in the existing mail servers. Security is one of the main parameters of the proposed system which is facilitated by using the three layer authentication techniques making it more secure and reliable when compared to the existing mail servers. Availability and the overall performance of the proposed system are almost similar to that of the existing systems. Limitations are that the mobile network range should be a must in order to receive original mail. Authentication and Confidentiality are significantly higher since the user logs in providing a valid user name and password which is the first level of security followed by the Encryption, Decryption, Divide and Merge processes which constitute the second level and the OTP generation is the third level of security provided by the developed system.

6. CONCLUSION

The proposed system overcomes the drawbacks found in the present existing mail servers regarding security by providing better security for the mails especially containing critical information. Hacking has become one of the greatest threats faced in today's mailing systems due to the usage of only one level of security, i.e., a login-password system. The developed application with 3 layer authentication provides enhanced security for the critical mails shared via Internet and ensures that the users don't have to worry about the message being hacked. It builds a secure system that will ensure that the critical information is not leaked or misused thus making it an ideal mailing system. It adds privacy, authentication, message integrity, and non-repudiation to plaintext email.

The future scope could be to enhance the system to support attachment of video and other type of files, facilitating message transmission to multiple recipients at a time as well as regeneration of the same OTP for multiple operations from a particular user.

7. REFERENCES

[1] Email Security - What Are The Issues? http://www.net-security.org/article.php?id=816

[2] Email: the forgotten security problem http://nakedsecurity.sophos.com/2012/11/07/email-systems-are-fundamentally-insecure/

[3] Security Issues and Solutions in Internet E-mail http://www.cuhk.edu.hk/itsc/network/app/email/security/securityissues.htm

[4] The Radicati Group, INC, A Technology Market Research Firm, Email Statistics Report 2013-2017, Available:http://www.radicati.com/wp/wpcontent/uploads/2013/04/Email - Statistics - Report - 2013 - 2017-Executive-Summary.pdf, Visited: 28 March 2013

[5] Giampaolo Bella, Cristiano Longo and Lawrence C Paulson,"Verifying Second-Level Security Protocols", Lecture Notes in Computer Science", Volume 2758, pp 352-366, Springer Berlin Heidelberg, 2003

[6] Dan Zhou, Joncheng C. Kuo, Susan Older and Shiu-Kai Chin, "Formal Development of Secure Email", HICSS-32. Proceedings of the 32nd IEEE Annual Hawaii International Conference on System Sciences, 1999, Maui, HI, USA

[7] M. Abadi and B. Blanchet, “Computer-Assisted Verification of a Protocol for Certified Email”, Static Analysis, 10th International Symposium (SAS’03), Volume 2694, pp. 316-335, Lecture Notes in Computer Science (LNCS),San Diego, California, June 2003. Springer Verlag.

[8] L. C. Paulson, “The inductive approach to verifying cryptographic protocols”, Journal of Computer Security, Vol. 6, 85 - 128, 1998.

[9] Martin Abadi, Neal Glew, Bill Horne and Benny Pinkas, “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, 2002.

[10] Brian Donadi, A Guide E-Mail Systems and Security, Available: http://www.infosecwriters.com/text_resources /pdf/BDona dio_Email.pdf.

[11] L. C. Paulson, “Inductive analysis of the internet protocol TLS”, ACM Transactions on Information and System Security, 2(3): 332 - 351, 1999.