Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

SECURE TRANSACTION SYSTEM

Priyanka S. Raut [1] , Laxmi K. Yelle [2] , Pranita S. Chore [3] , Susmit S. Bhele [4] , Sameer A. Thakre [5] , Pranita P. Deshmukh [6]

[1] Computer Science & Engineering, PRMIT&R, Badnera.

[2] Computer Science & Engineering, PRMIT&R, Badnera

[3] Computer Science & Engineering, PRMIT&R, Badnera

[4] Computer Science & Engineering, PRMIT&R, Badnera

[5] Computer Science & Engineering, PRMIT&R, Badnera

[6] Assistant Professor, Computer Science & Engineering, PRMIT&R, Badnera

Abstract

Encryption is an essential tool for protecting the confidentiality of data. Network security protocols such as SSL or IPSec use encryption to protect Internet traffic from eavesdropping. Encryption is also used to protect sensitive data before it is stored on non-secure disks or tapes. Encryption, however, is computationally expensive. A computer server that must encrypt data for thousands of clients before sending it over the network can easily become crypto-bound. The capacity of the server is then determined by the speed at which it can perform encryption. DES and Triple-DES are very widely used, it is important to optimize the performance of these algorithms. Triple-DES (TDES) is basically used in various cryptographic applications and wireless protocol security layers. The main objective of the project is to provide secured communication.

Keyword – DES, Triple DES, Encryption, Decryption

1. INTRODUCTION

Electronic mail known as Email has evolved significantly throughout the years, emerging as the central means of communication. System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. The security is playing a very important and powerful role in the field of networking, Internet and various communication system .The electronic communication system is used in banking, reservation system and marketing which required a very tight security system. However once misused, email based communication may carry various disadvantages

- An unsecure email is threat to one's organizational security, as it contains the private information about particular organization.

- An unsecure email is also dangerous for one's privacy, as it is unsecure form the third party hacker.
- An unsecure email could not maintain the data confidentiality, as no encryption is performed on the email.
- With the use of unsecured email there are chances of sensitive data leakage with no possibility of tracking.

So to overcome these problems we have designed an system that provides the security and confidentiality by using Triple-DES algorithm.

Triple-DES is proposed by IBM in 1978 as a substitute to DES. So, 3DES is simply the DES symmetric encryption algorithm, used three times on the same data. Three DES is also called as T-DES. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text. The Brute Force attack is weak against the 3DES because the intruder required breaking the DES and Simple Columnar Approach both. He required extra time to hack the algorithm. If the intruder is success to hack the key of DES in any way then he required the random number of the columnar approach to reach the plain text.

The original DES implementation has some weaknesses, to overcome the most of weakness the 3DES algorithm is designed. The Designed system improved the security power of original DES. Main aim is to enhance the security of a system. By using the 3DES algorithm the security is very tight and approximately impossible to crack and break the 3DES algorithm. When it was discovered that a 56-bit key of DES is not enough to protect from attacks, TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys.

3DES which is DES with three different keys. It is essential to avoid having the same key for the encryption steps since the output will only be a slower version of DES. 3DES has two forms, one requiring three completely different keys and the other only two completely different keys. The first method uses three keys to encrypt the plaintext, firstly using key k1, followed by encryption with key k2, and lastly a third encryption is carried out with key k3. We perform the operation C = EK3(EK2(EK1(P))) to encrypt the plaintext and P = DK3(DK2(DK1(C))) for decryption. PGP and S/MIME are examples of products that use the three keys 3DES. Even though 3DES uses three keys to provide a high level of security, it still has a drawback since its required 56 * 3 = 168 bits for the keys, which can be difficult to make work in practical situations. Because of this, the method of 3DES using two keys has arisen. In 3DES with two keys, encryption is applied using key k1, the output of the previous step is decrypted using key k2. Finally, encryption of the output of step 2 is encrypted again using key k1. We perform the operation C = EK1(DK2(EK1(P))) to encrypt the plaintext and P = DK1(EK2(DK3(C))) for decryption. This method is also referred to as Encrypt- Decrypt- Encrypt (EDE).

There are several application and websites available for an online communication on the web. In order to make communication more secure and to increase the interaction between students and teachers staff we are coming up with (secure transaction system).Where authenticate user can share documents securely and students can show their extra curriculum activities. Also T&P department able to notify student about placement notices and different workshops.

Secure Transaction System as name suggest is an web application to mailing system which is used to send and receive messages. The aim to develop such web application is to support secure communication such as compose application, inbox application, blog application to show student curriculum and T&P notification etc.

2. LITERATURE REVIEW/SURVEY

Giampaolo Bella et al. 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 formalize such concepts as sending a confidential message, an authenticated message, or a message with guaranteed delivery [1].

According to the Radicati Group's study, "Microsoft Exchange and Outlook Analysis, 2005-2009," 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 [2].

M. Abadi et al. 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 [3].

Martin Abadi et al. 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. [4]

Brian Donadi 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 [5].

D. S. Abdul. Elminaam et.al., (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices in their paper named "Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices." following points are concluded by him from his experimental result. 1) If packet size is changing with or without transmission of data using various WLANs protocols and different architectures. It was concluded form the result that Blowfish and 3DES has better performance than other common encryption algorithms such as DES and RSA [6].

Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, "A New Modified Version of 3DES Based Algorithm for Image Encryption" (2010) The authors proposed an enhanced model of DES to possess good level of security and better range of image encryption. The modification process can be carried out by adjusting the Shift Row Transformation. As the result shown, that the comparison has been made in between the original 3DES encryption algorithm and the modified algorithm which produces very good encryption results focusing towards the security against statistical attacks[7].

3. SYSTEM ARCHITECTURE

3.1 Existing System

The existing email system is emerging as the central means of communication. Today's email systems are based on a `store-and-forward' model. As Email `servers' accept, forward, deliver and store messages, neither the sender nor the recipients' online physical presence is necessary simultaneously. The sender can enter the messages and the recipient can retrieve it whenever he/she is free. An important advantage of it is the reduction of consumption of papers in office. Nowadays trade and commerce have been dependent on this speedy mode of communication to a great extent giving us an opportunity to face the international dome. E-mail has lot of advantages to its credit establishing world wide information network with remote areas of the earth.

The attachments or mail content forwarded with the email are insecure in today's mailing system. After misemployed, the communication based on the email may carry some demerits and even hazardous for one's organizational security, privacy and data confidentiality. Considering these serious challenges, the importance of protecting sensitive email data is clear and crucial.

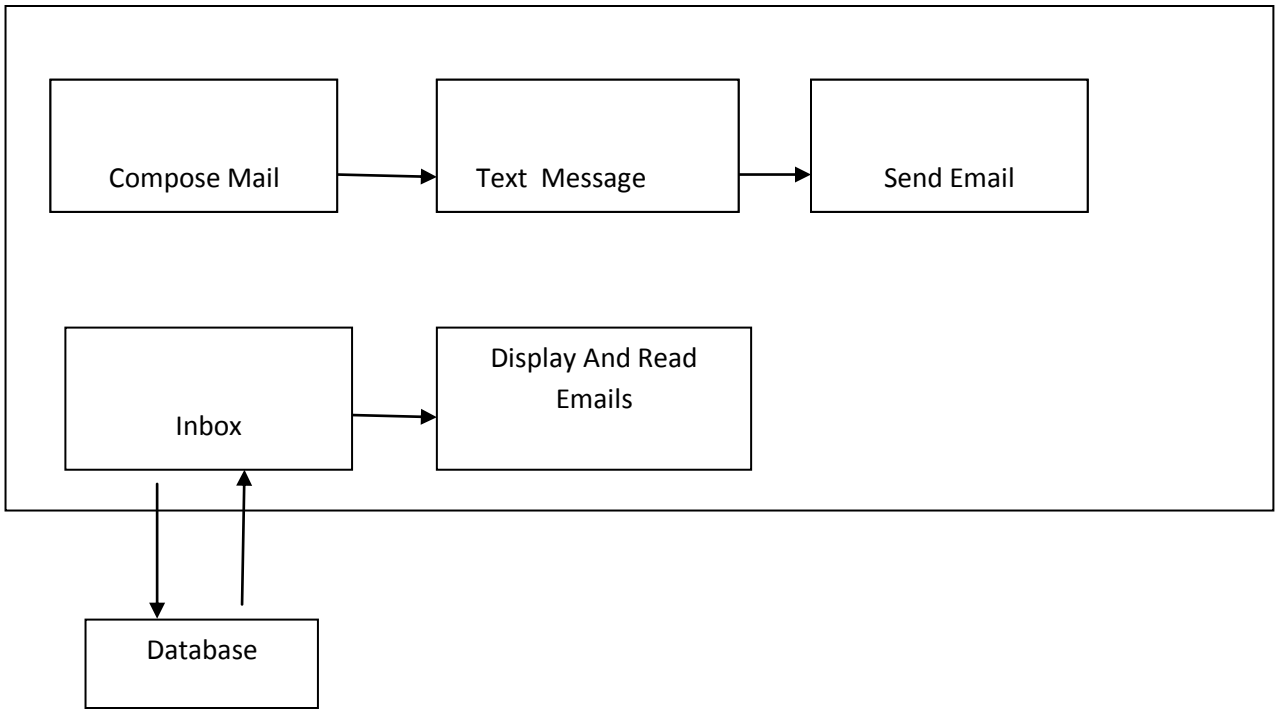

Fig 3.1. Existing Email System

3.2 Proposed System

The users of Secure Transaction System are given a unique login id and must give the correct password. It gives total security for us. So unauthorized user can't allow accessing the messages. The main advantage of the Secure Transaction System is it security feature allowing only registered users to access the system and it uses 3DES algorithm for message encryption preventing any hackers to access messages.
As the access for Secure Transaction System is only restricted to the people registered within the organization itself and information is transferred within the organization itself, and all this transformation will be up to some limit so the data transformation will be fast.

3.3 Design Web Application

To design a Secure transaction System

- User Registration
- Login
- Inbox will list all received messaged
- Compose option will accept mail to be send & send the mail to appropriate user.
- Attachments can be sending with mail.
- It will show if a mail has been opened by receiver or not.
- Interaction with teachers
- Uploading extra curriculum activities eg.Blog
- Providing notification to students about college activities

4. SYSTEM DESIGN (ARCHITECTURE/BLOCK DIAGRAM, DFD, ALGO, ETC.)

4.1 DES

Data Encryption Standard (DES) is a cryptographic standard that was proposed as the algorithm for the secure and secret items in 1970 and was adopted as an American federal standard by National Bureau of Standards (NBS) in 1973. DES is a block cipher, which means that during the encryption process, the plaintext is broken into fixed length blocks and each block is encrypted at the same time.

Basically it takes a 64 bit input plain text and a key of 64-bits (only 56 bits are used for conversion purpose and rest bits are used for parity checking) and produces a 64 bit cipher text by encryption and which can be decrypted again to get the message using the same key. Additionally, we must highlight that there are four standardized modes of operation of DES: ECB (**E**lectronic **C**ode**b**ook mode), CBC (**C**ipher **B**lock **C**haining mode), CFB (**C**ipher **F**eed**b**ack mode) and OFB (**O**utput **F**eed**b**ack mode).

ECB: Electronic Code Book (ECB) is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding cipher text value and vice versa. In other words, the same plaintext value will always result in the same cipher text value.

CBC: Cipher block chaining (CBC) is a mode of operation for a block cipher (one in which a sequence of bits are encrypted as a single unit or block with a cipher key applied to the entire block). Cipher block chaining uses what is known as an initialization vector (IV) of a certain length.

CFB: Cipher text feedback (CFB) is a mode of operation for a block cipher. In contrast to the cipher block chaining (CBC) mode, which encrypts a set number of bits of plaintext at a time, it is at times desirable to encrypt and transfer some plaintext values instantly one at a time, for which cipher text feedback is a method. Like cipher block chaining, cipher text feedback also makes use of an initialization vector (IV). CFB uses a block cipher as a component of a random number generator. In CFB mode, the previous cipher text block is encrypted and the output is XORed (see XOR) with the current plaintext block to create the current cipher text block. The XOR operation conceals plaintext patterns. Plaintext cannot be directly worked on unless there is retrieval of blocks from either the beginning or end of the cipher text.

OFB: In cryptography, output feedback (OFB) is a mode of operation for a block cipher. It has some similarities to the cipher text feedback mode in that it permits encryption of differing block sizes, but has the key difference that the output of the encryption block function is the feedback (instead of the cipher text). The XOR (exclusive OR) value of each plaintext block is created independently of both the plaintext and cipher text. It is this mode that is used when there can be no tolerance for error propagation, as there are no chaining dependencies. Like the cipher text feedback mode, it uses an initialization vector (IV). The Changing IV in the same plaintext block results in different cipher text.

4.2 DES Algorithm

[1] In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.

[2] The Initial permutation is performed on plain text.

[3] The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).

[4] Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key:

- From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.
- Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.
- Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step.
- Using the S-box substitution produced the 32-bit from 48-bit.
- These 32 bits are permuted using P-Box Permutation.
- The P-Box output 32 bits are XORed with the LPT 32 bits.

- The result of the XORed 32 bits are become the RPT and old RPT become the LPT. This process is called as Swapping.
- Now the RPT again given to the next round and performed the 15 more rounds. After the completion of 16 rounds the Final Permutation is performed.

4.3 Flowchart

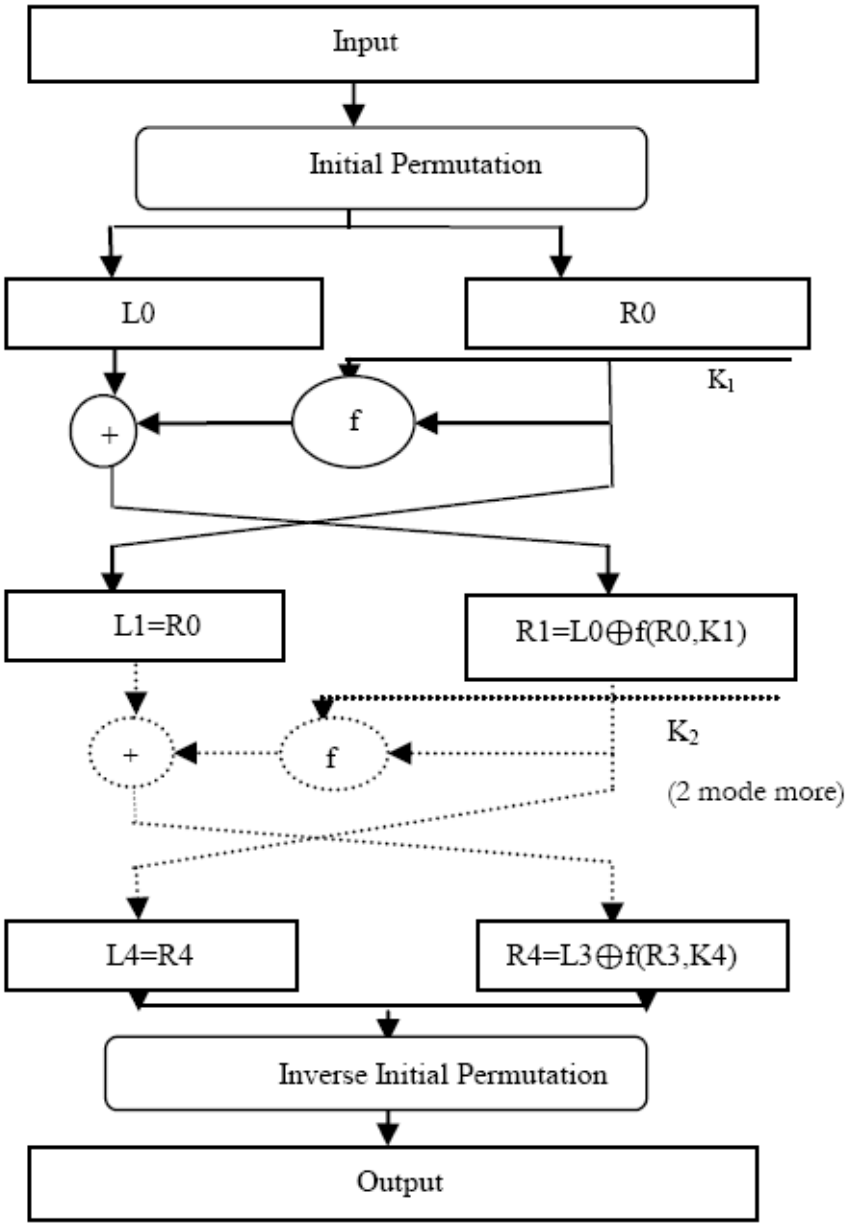

Fig. 1: DES Fiestel Diagram

4.4 Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows –

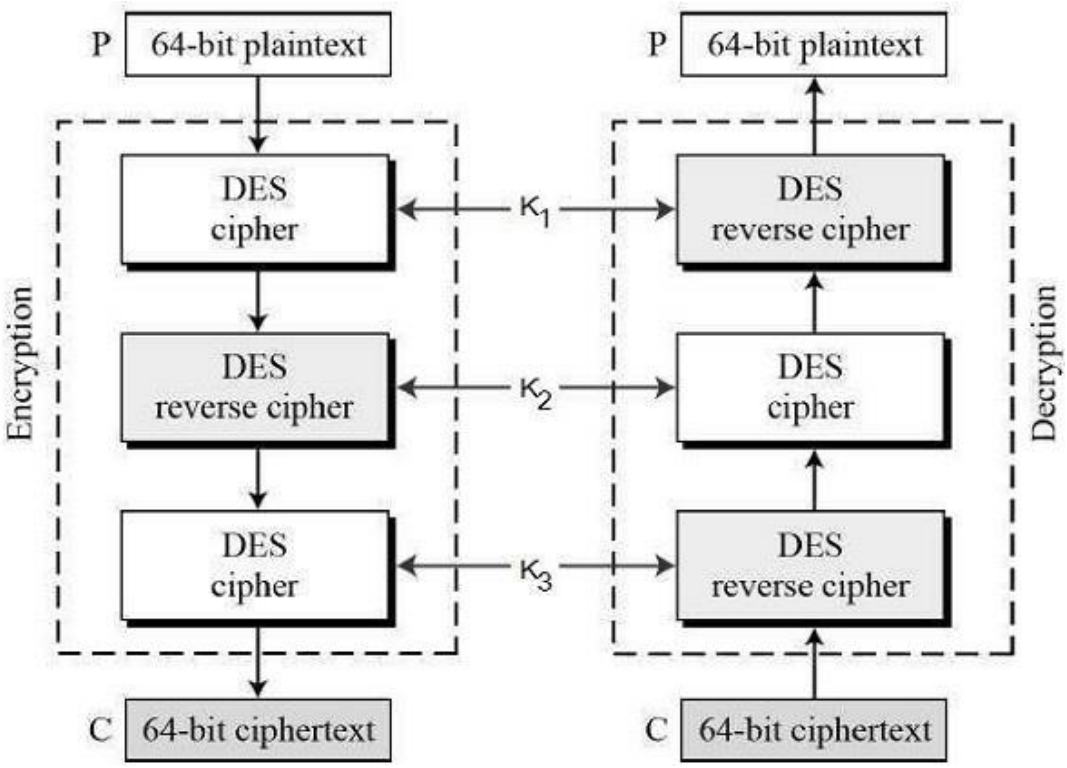

Fig.4.4. Encryption Scheme

- **Encryption Scheme**

The encryption-decryption process is as follows −

1. Encrypt the plaintext blocks using single DES with key K1.
2. Now decrypt the output of step 1 using single DES with key K2.
3. Finally, encrypt the output of step 2 using single DES with key K3.
4. The output of step 3 is the cipher text.
5. Decryption of a cipher text is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.
6. Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

7. Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. Therefore, 2TDES has a key length of 112 bits.
8. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

4.5 Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modelling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

A DFD shows what kind of information will be input to and output from the system, how the data will advance through the system, and where the data will be stored. It does not show information about the timing of process or information about whether processes will operate in sequence or in parallel unlike a flowchart which also shows this information.

Larry Constantine, the original developer of structured design, based on Martin and Estrin's "Data Flow Graph" model of computation. Starting in the 1970s, data flow diagrams (DFD) became a popular way to visualize the major steps and data involved in software system processes. DFDs were usually used to show data flow in a computer system, although they could in theory be applied to business process modeling. DFD were useful to document the major data flows or to explore a new high-level design in terms of data flow.

Data flow diagrams are also known as bubble charts.[5] DFD is a designing tool used in the top-down approach to Systems Design. This context-level DFD is next "exploded", to produce a Level 1 DFD that shows some of the detail of the system being modeled. The Level 1 DFD shows how the system is divided into sub-systems (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

Data flow diagrams are one of the three essential perspectives of the structured-systems analysis and design method SSADM. The sponsor of a project and the end users will need to be briefed and consulted throughout all stages of a system's evolution. With a data flow diagram, users are able to visualize how the system will operate, what the system will accomplish, and how the system will be implemented. The old system's dataflow diagrams can be drawn up and compared with the new system's data flow diagrams to draw comparisons to implement a more efficient system. Data flow diagrams can be used to provide the end user with a physical idea of where the data they input ultimately has an effect upon the structure of the whole system from order to dispatch to report. How any system is developed can be determined through a data flow diagram model.

In the course of developing a set of levelled data flow diagrams the analyst/designer is forced to address how the system may be decomposed into component sub-systems, and to identify the transaction data in the data model.Data flow diagrams can be used in both Analysis and Design phase of the SDLC. There are different notations to draw data flow diagrams (Yourdon & Coad and Gane & Sarson), defining different visual representations for processes, data stores, data flow, and external entities.

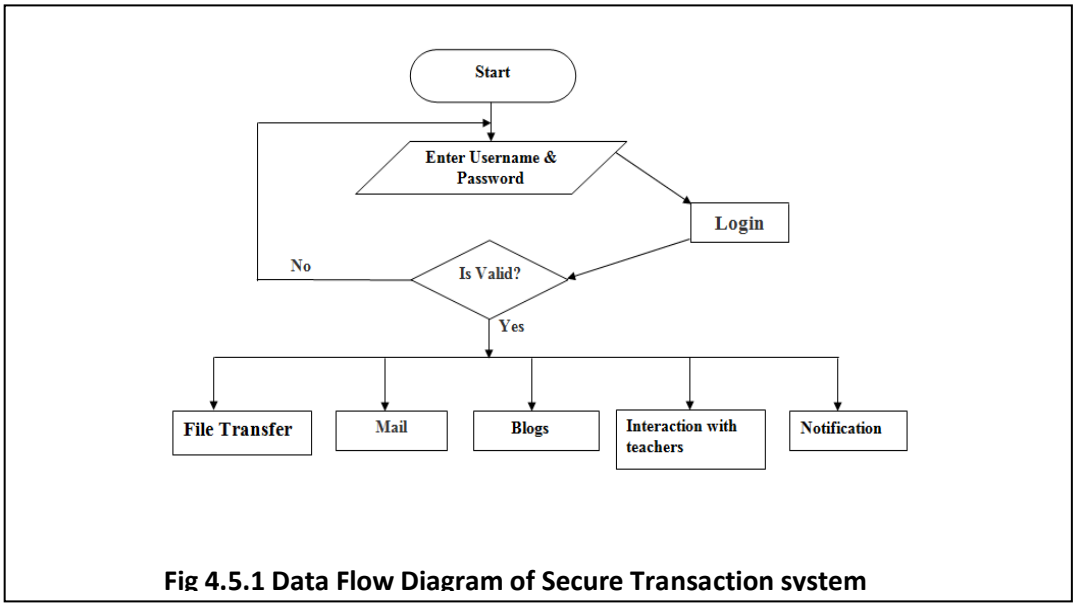

Fig 4.5.1 Data Flow Diagram of Secure Transaction system

Above figure c. shows data Flow diagram of Secure transaction System. Where registered user will enter his/her email id and password. If user is authorized then user can transfer file, send mail, write or read blogs and able to interact with teachers etc.

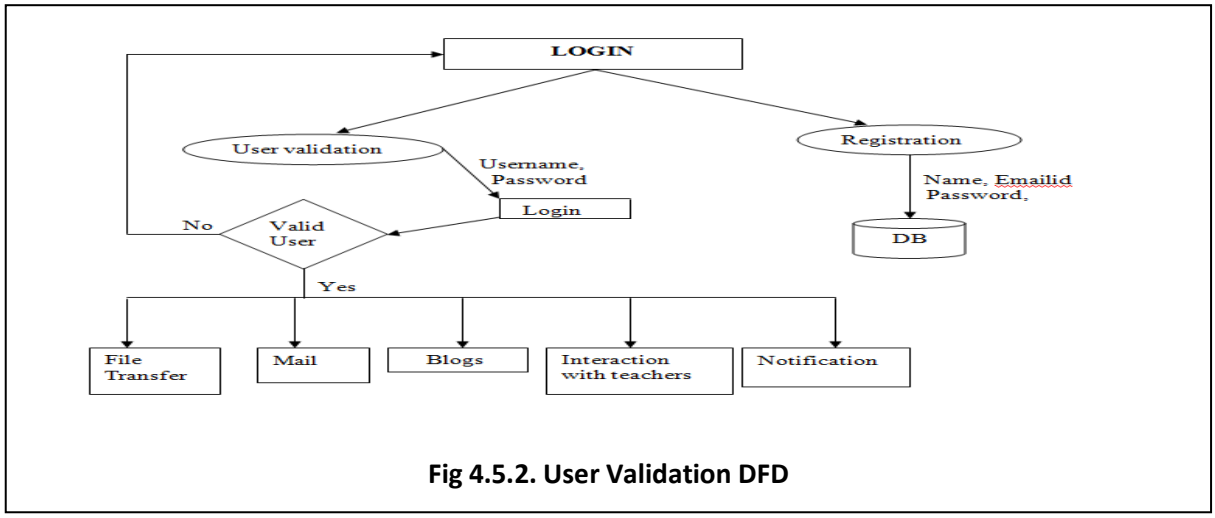

Fig 4.5.2. User Validation DFD

Above figure shows DFD of user validation. Before Login user has to register itself with parameters such as name, email id password etc. After registering user can login into the system and get access of application facility.

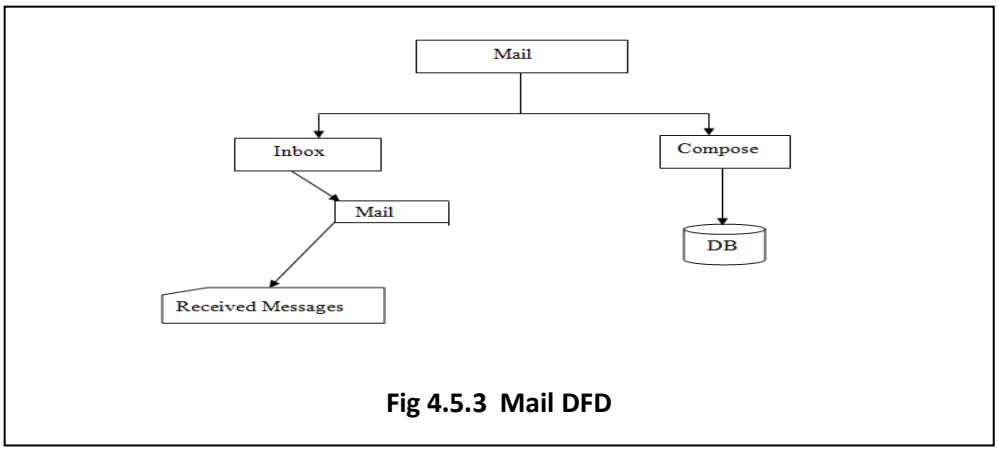

Fig 4.5.3 Mail DFD

Above figure c. shows the DFD of mail. User can send mail to another user. Inbox

Above figure e. shows received mails where compose allow to send mail to user.

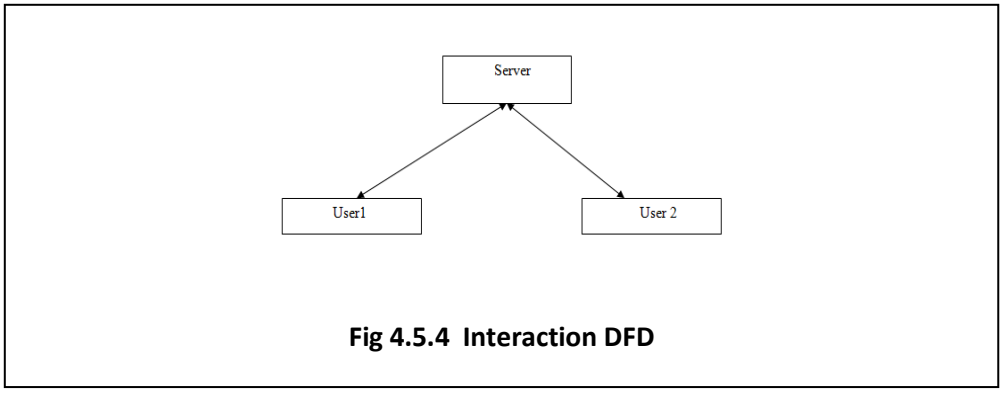

Fig 4.5.4 Interaction DFD

Above figure f. shows DFD of Interaction between to user.

5. IMPLEMENTATION & RESULTS

The user of Secure Transaction System is given a unique login id and must give the correct password. It gives total security for us. So unauthorized user can't allow to see our messages. The main advantage of the Secure Transaction System is it's security feature allowing only registered users to access the system and it uses 3DES algorithm for message encryption preventing any hackers to access messages. As the access for Secure Transaction System is only restricted to the people registered within the organization itself and information is transferred within the organization itself, and all this transformation will be up to some limit so the data transformation will be fast.

5.1 Home Page

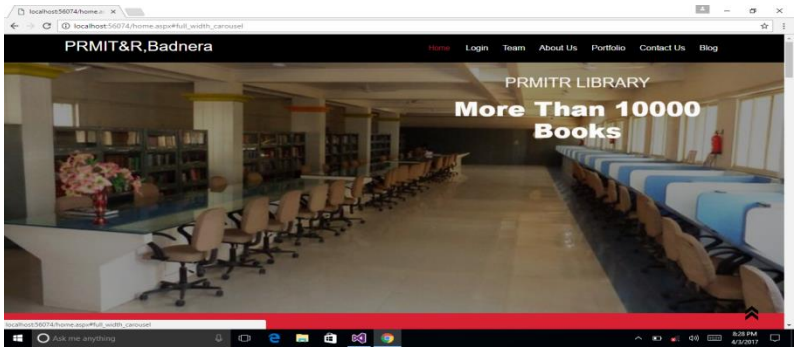

Fig.5.1.1 Home Page

A home page or a start page is the initial or main web page of a website or a browser. The initial page of a website is sometimes called main page as well. A home page is generally the main page a visitor navigating to a website from a web search engine will see, and it may also serve as a landing page to attract visitors. The home page is used to facilitate navigation to other pages on the site by providing links to prioritized and recent articles and pages, and possibly a search box. Home page of this project have link of Login, Portfolio, Contact, Blog etc.

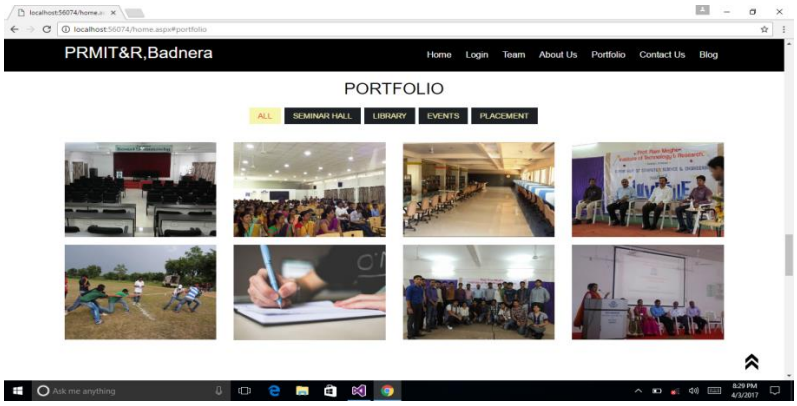

Fig.5.1.2 Portfolio

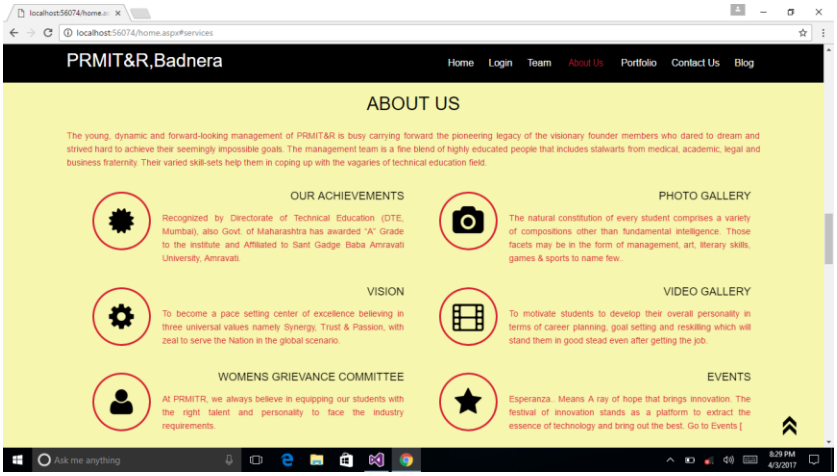

Fig.5.1.3 About College

Portfolio figure 5.1.2. and 5.1.3. shows photos where as contact us tab shows information about college to new user.

5.2 Idea of Registration

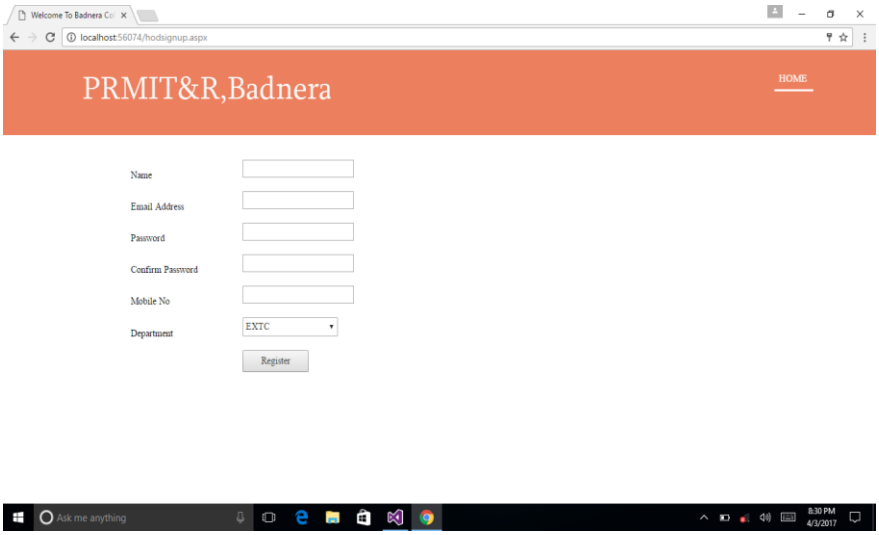

Fig 5.2.1 Registration

In registration page the user have to fill the form by selecting username, email address, password, mobile number and department. After filling the form, click on register button. If user successfully register then user able to login.

5.3 Idea of Login Phase

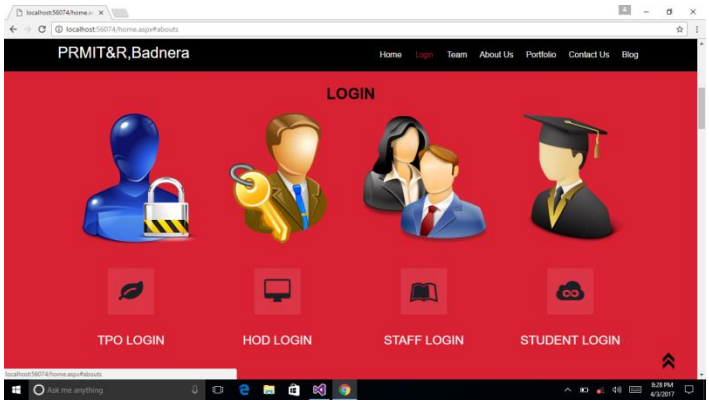

Fig.5.3.1 Login Page

In computer security, logging in, (or logging on or signing in or signing on), is the process by which an individual gains access to a computer system by identifying and authenticating themselves. The user credentials are typically some form of "username" and a matching "password" and these credentials themselves are sometimes referred to as a login, (or a logon or a sign in or a sign on). From this page of project user can log in into site according to user position.

Fig.5.3.2 HOD, Staff Login Page

Figure 5.3.2, shows login page for HOD. Authenticate HOD (user) login and have rights to activate or deactivate teacher staff and can interact with student and staff via mailing. Figure 7. shows login page for staff. Authenticate staff (user) login and have rights to activate or deactivate students can interact with student via mailing. Authenticate student (user) login can interact with TPO, HOD and teachers via mailing.

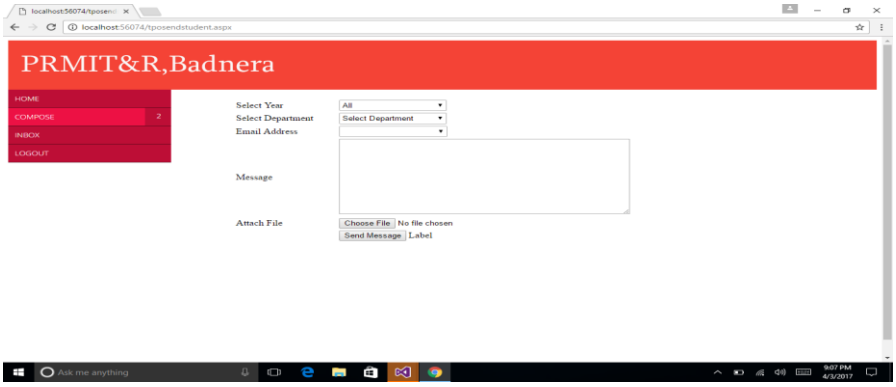

Fig.5.3.5 Compose

You can compose and send your email messages as soon as you write them; In the To text box, enter the email addresses of the person or persons to whom you are sending the message.

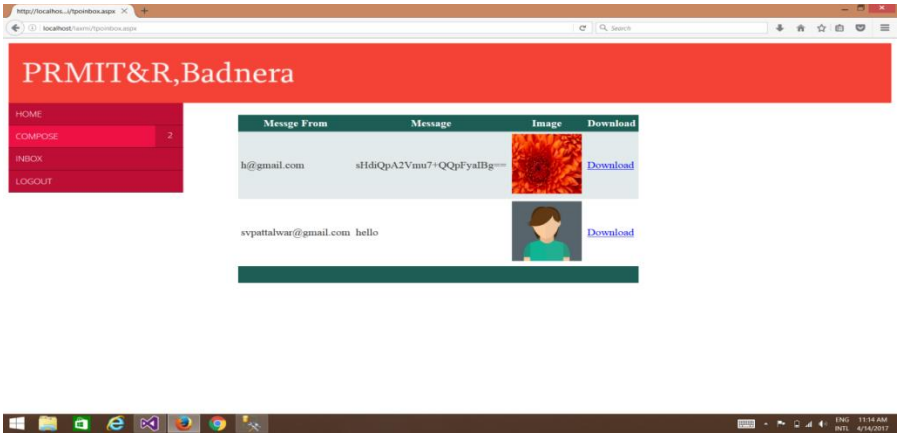

Fig 5.3.6 Inbox

INBOX is the name given to the folder where your newly-delivered email messages appear. The Inbox is opened when you login and c lick on inbox to read your email. Your Inbox is designed to act only as a delivery point and should not be used for permanent storage of email.

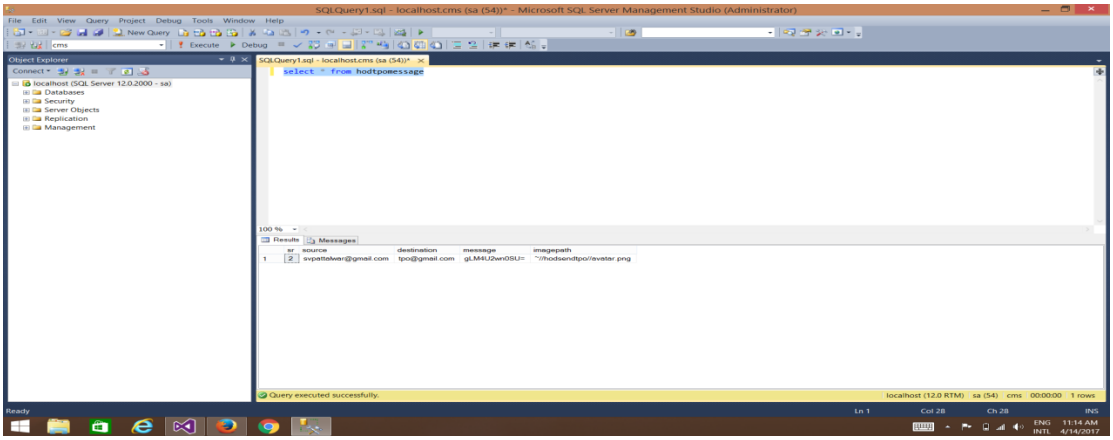

Fig 5.3.7 Encryption of message

Figure5.3.7 shows message which are send by users and it is in encryption form.

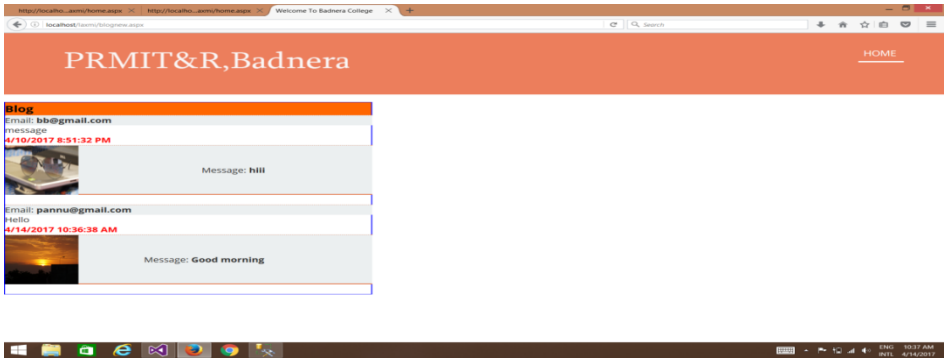

Fig.5.3.8 Blog

A blog is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries ("posts"). Posts are typically displayed in reverse chronological order, so that the most recent post appears first, at the top of the web page.

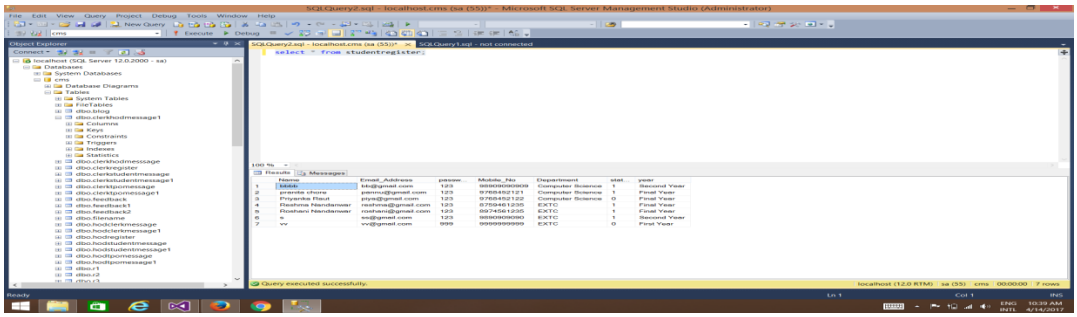

Fig 5.3.9 Database

Figure 5.3.9. shows database. It contains user information those who are register.

6. CONCLUSION AND FUTURE SCOPE

The proposed system provides 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 provides more 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 by using 3DES algorithm.

Thus in this project every user need authentication to login. As admin will authenticate HOD, HOD will authenticate Teachers, Teachers will authenticate students. Where all the users of application can communicate via secure mailing such as sending notices, notifications regarding T&P and college, assignments and curriculum activity.

The project will be more users friendly with the future enhancement of having the verification mails, warning mails and news updates to be send to the using the automatic mailing facility, online assignment submission and displaying result of student, attachment of video etc. The enhancement also consists of making private chat more effectively and making blog facility more effective.

7. REFERENCES

[1] 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

[2] 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

[3] 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.

[4] 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.

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

[6] Simar Preet Singh, and Raman Maini "Comparison of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol.2, No. 1, January-June 2011, pp. 125-127.

[7] Network Associates, "PGP Freeware for Windows 95, Windows 98,Windows NT, Windows 2000 & Windows Millennium User's Guide Version 7.0", available from http://www.pgpi.org/doc/guide/7.0/en/win/, 2001
.

[8] Housley, R., W. Ford, W.Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL profile", RFC 2459, 1999.

[9] Stallings, W., "Cryptography and Network Security, 3/E", Chapter 11, Prentice Hall, 2003.

[10]J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[10] National Institute of Standards and Technology (NIST), "FIPS Publication 46-2: Data Encryption Standard", 1993.

[11] National Institute of Standards and Technology (NIST), "FIPS Publication 180-1: Secure Hash Standard", 1995.

[12] Krawczyk, H., M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC2104, 1997.

[13]Levi A., "How Secure is Secure Web Browsing", Comm. of the ACM, vol. 46, no. 7, pp. 152, July 2003.

[14] E. Gerck. Secure Email Technologies X.509/PKI, PGP, IBE and ZMAIL: A us- ability and security comparison, pages 171–196. ICFAI University Press, 2007.

[15] M. Tracy, W. Jansen, K. Scarfone, and J. Butterfield. Guidelines on electronic mail security. Technical report, National Institute of Standards and Technology, 2007.