International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

# Secure Gmail Communication Implementation Using Encryption Layer

M. Surya Prakash[1], B. Mahender Reddy[2], S.Rajesh[3]

[1] B. Tech Scholar, Department of Computer Science Engineering, Siddhartha Institute of Engineering and Technology, Vinobha Nagar, Ibrahimpatnam, Hyderabad, Telangana 501506.
[2] Associate Prof., Department of Computer Science Engineering, Siddhartha Institute of Engineering and Technology, Vinobha Nagar, Ibrahimpatnam, Hyderabad, Telangana 501506.
[3] Asst. Prof., Department of Computer Science Engineering, Siddhartha Institute of Engineering and Technology, Vinobha Nagar, Ibrahimpatnam, Hyderabad, Telangana 501506.

**ABSTRACT-** The core idea behind our project is to maintain the information in secure way over the e-mail communication. In generally when the user is sending information over the email, the entered information will be passing as a text to the destination, in this process there is a chance to hack the information as we are seeing in real time, hence the information needs to be protected. Data Security is a primary concern for every communication system. There are many ways to provide security to data that is being communicated. This project describes a design of effective security for communication by AES algorithm for encryption and decryption.

In our project the data will be converted into encrypted format and then the encrypted information is sent to the receiver email, if the receiver wants to access the information the user decrypts , entire encrypted information will convert into plain text automatically. In this entire process we are using private key and public key for encryption and decryption process for providing more security.

## I. INTRODUCTION

### 1.1 THE GROWING IMPORTANCE OF GMAIL

Nowadays sending mails throughout the world is being a major demand in business. People prefer Gmail for sending mails, since it provides a free Internet not supported by ads or corporate revenues, but rather the free exchange of ideas.

The concern is to provide security to mails such that foil sniffers who sit in cafes, eavesdropping in on traffic passing by. And this discovers concerted attempts to break into Gmail accounts of human right activists. The switch to always-on HTTPS adds more security, but does not help this kind of attacks.

The existing system which we use is mailing through computer using internet which is not secure. Gmail is largely used as search engine for mailing. There are many users across the world that prefers Gmail over other search engines for mailing. So there is a possibility that that foil sniffers who sit in cafes, eavesdropping in on traffic passing by. And this discovers concerted attempts to break into Gmail accounts of human right activists. The switch to always-on HTTPS adds more security, but does not help this kind of attacks.

Now-a-days as technology is increasing usage are also increasing so mailing emails costs an individual higher and internet may not be secure at the place where he is residing these are some of the drawbacks of the existing system.

This paper presents a method to make sending information requested by users in Gmail is more safe and secure based on the idea of Encryption.

By hiding information in email and lack of direct sending of information, this method increases the security of sending the information for users in Gmail.

Some of the reasons for preference of encryption layer over Gmail communication are

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

No mail knowledge for sniffers;
High penetration coefficient;
Fully personalized; and
4-Provide Security.
Used to increase the convenience of the Gmail users and reduces security cost.

## II. LITERATURE SURVEY

### 2.1 INTRODUCTION

Encryption is one of the fundamental ways by which data can be kept confidential. This article will offer a brief introductory discussion of encryption: what it is, how it can be used, and the true implications it can have on information security.

### 2.2 AES ALGORITHM

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.[4]
The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

### OPERATION OF AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).[6]
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −
The schematic of AES structure is given in the following illustration −

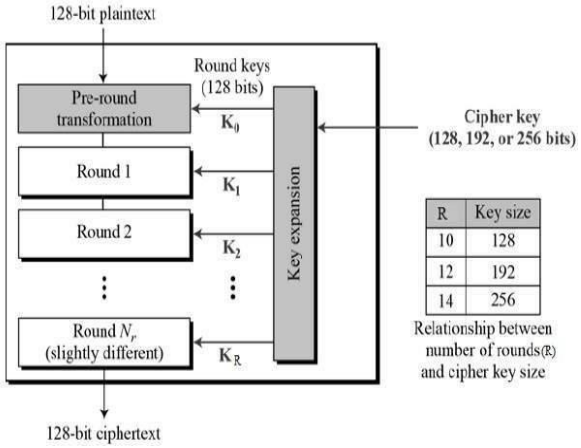


**Fig 2.1 AES Structure**

In fig 2.1, Unlike DES[7],, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

**Encryption Process**

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes.

**Byte Substitution(Sub Bytes)**

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

**Shiftrows**

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −
Fourth row is shifted three positions to the left.
The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

**Mixcolumns**

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

**Addroundkey**

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

**Decrytion Process**

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

Add round key
Mix columns
Shift rows
Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

### 2.3 AES ANALYSIS

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered.[8]

## III. SYSTEM ANALYSIS

### 3.3 PROPOSED SYSTEM

The proposed system intends to implement an encrypted layer in Gmail communication which encrypts the data before it is transmitted so as to protect the information from being hacked. Starting this process would provide a safer internet.

### 3.4 ADVANTAGES OF PROPOSED SYSTEM

The proposed system allows user to eliminates above problems . In this application the data will be converts into encrypted format and we are sending that encrypted format information to the receiver email, there if he wants to see the information we are providing one option to the user that is decryption whenever the user will press that automatically the entire encrypted information will convert into plain text.

### 3.5 ANALYSIS MODEL

The model that is basically being followed is WATER FALL Model which states that the phases are organized in a linear order. First of all, the feasibility study is done. Once that part is over, the requirement analysis and project planning begins. If system exists as a whole but modification and addition of new module is needed, analysis of present system can be used as basic model.

The design starts after the requirement analysis is complete and the coding begins after the design is complete. Once the programming is completed, the testing is done.

Here the linear ordering of these activities is critical. At the end of the phase, the output of one phase is the input to other phase. The output of each phase should be consistent with the overall requirement of the system. Some of the qualities of spiral model are also incorporated like after the people concerned with the project review completion of each of the phase the work done.

**Water Fall Model:-** In fig 3.1WATER FALL Model has been chosen because all requirements were known before and the objective of our software development is the computerization/automation of an already existing manual working system.

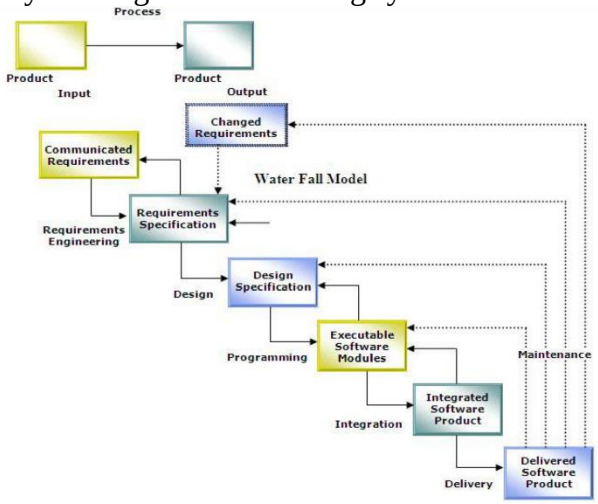


**Fig. 3.1: Water Fall Model**

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

## IV. SYSTEM IMPLEMENTATION

**MODULES**

There are mainly four modules
User authentication
Mailing Module
Public/Private key generation
Encryption/Decryption

**User Authentication Module**

This module is used for identifying the user and verifying that the user is allowed to access some restricted service.
It accepts the username and password provided by the user and verifies it by comparing it with the values stored in the database.
It checks whether the user has the authority to access the certain service.
This module is developed by JSP.

**Mailing Module**

In this module, a user can send the data to other mail.
When he is transferring the data from his account, the entire message body is converted into encrypted format and then it sends to the other mail.
The receiver must be registered to decrypt the encrypted message.

**Private Key Generation Module**

In this module, the public key and the private key are generated using the AES algorithm.
AES stands for Advanced Encryption Standard.
It is an algorithm for public-key cryptography. [5]
It is the algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography..

**Encryption / Decryption**

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is **encrypted** information (in cryptography, referred to as ciphertext).

- I
In this module, while sending the message, the information is transformed into encrypted format with the help of a key and then it is sent to the other account.
- T
The person who received the mail should decrypt it every time to see the actual content.
- F
For the purpose of decryption, a private key is used. In order to decrypt the data, the receiver must know the private key.
- T
The private key is generated by the server and it is sent to the receiver securely.

## V. RESULTS

**OUTPUT SCREENSHOTS**

**Login Page**

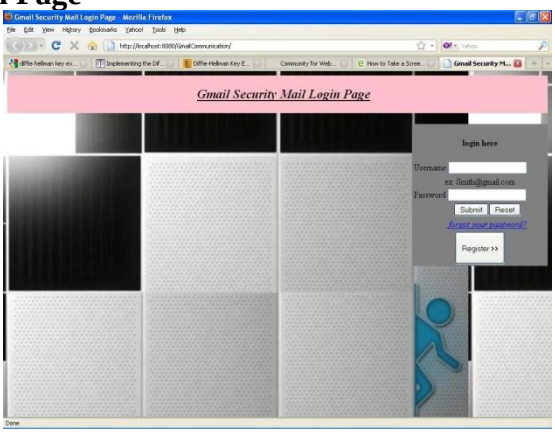


**Fig.5.1: Gmail security mail login page**

The login page of the Gmail Security Mail Login Page where the registered user can login and send an encrypted message to the other .

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

**Registration Page**


**Fig5.2: Register page**

The Registration Page where the user can register and then he/she logins into the Gmail Security Mail and where he/she can encrypt or decrypt a message.

**Re-register Page**

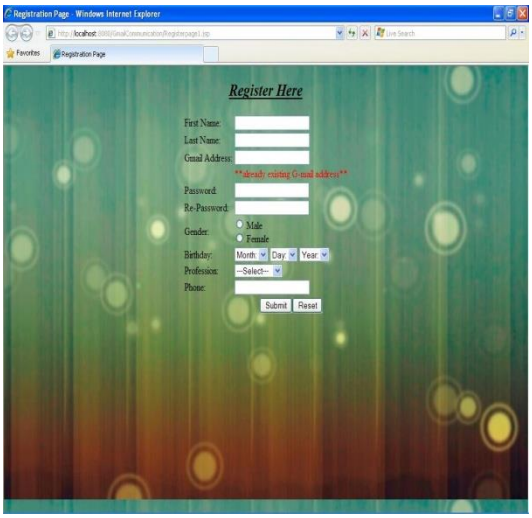


**Fig5.3: Re-registration page**

Fig. refers to registration of the user to provide a valid G-mail address.

**Recovery Page**

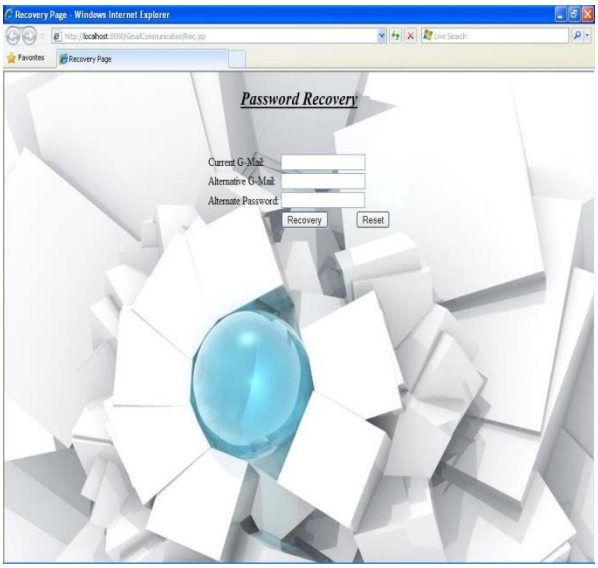


**Fig.5.4: Password recover page**

Fig. refers to the Password Recovery Page where if the user has forgot his/her password then he can recover it by providing a G-MAIL account name he/she is using currently and a message is sent to him/her with password recovery details.

**Send Mail**

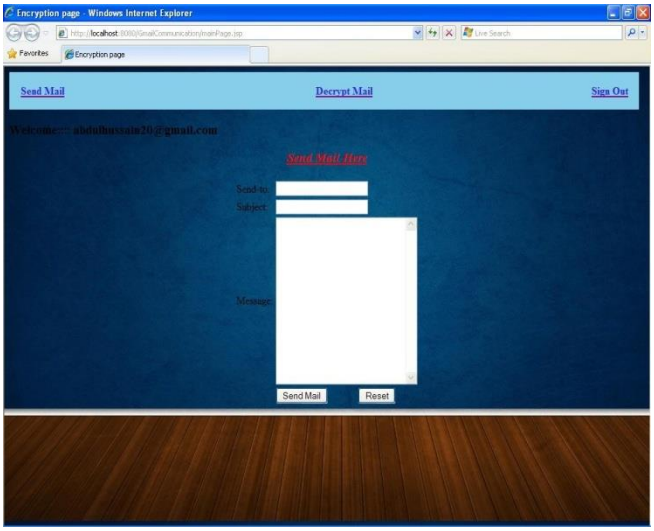


**Fig5.5: Send Mail page**

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 3
March 2017

Fig refers to the page where a registered user who has logged into the Gmail Security Mail Page and provides the account name to whom he/she wants to send a message ,then he/she will encrypt the message and will send the mail.

**Decrypt Mail Page**

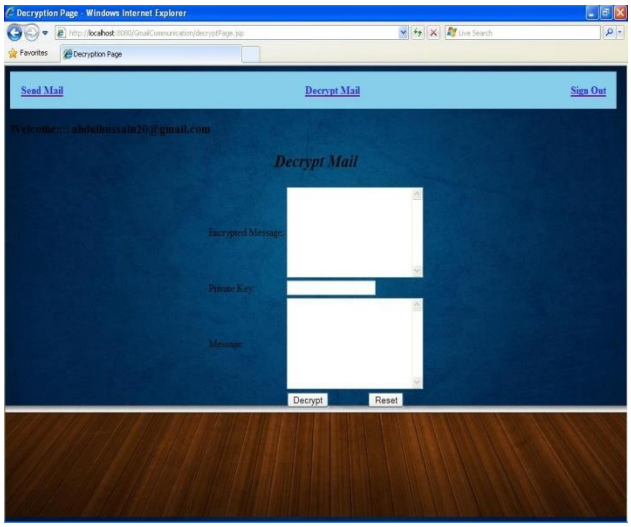


**Fig5.6: Decrypt Mail Page**

Fig refers to a page of the receiving end where the user who has received an encrypted message decrypts it and reads the message.

## VI. CONCLUSIONS AND FUTURE ENHANCEMENTS

Implementation of encrypted layer over Gmail communication is a web application which is solely used for protecting the confidentiality of the messages passed over the internet. Any registered Gmail user can use this application which allows the secured transmission of data.

In this world of internet encryption of every data is the basic need of all communication systems. Tremendous change in technology will appear if this solution is free of cost. Today mobile phones are most important and habitual thing for each human being. In the same way this encryption technology will become the basic need of everyone.

Due to increasing use of computers, now a day security of digital information is most important issue. Intruder is an unwanted person who reads and changes the information while transmission occurs. This activity of intruder is called intrusion attack. To avoid such attack data may be encrypted to some formats that is unreadable by an unauthorized person. AES is mainly advance version of data encryption standard (DES).[10][11]

Before going into the future enhancements as we came to know that cryptography can also be performed with not only the messages but also with audio file, within attachments etc. so in our future enhancements we can implement in the audio file. We can embed the attachment into encrypted format so that we can provide better security for attachments.

Additionally, AES has built-in flexibility of key length, which allows a degree of 'futureproofing' against progress in the ability to perform exhaustive key searches.However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

## REFERENCES

[1].http://www.cryptography.com

[2]. AES page available via http://www.nist.gov/CryptoToolkit.

[3].http://www.virtualschool.edu/mon/Crypto/

[4]. William Roche, "The Advanced Encryption Standard, The Process, Its Strengths and Weaknesses", University of Colorado, Denver, Spring 2006 Computer Security Class, CSC 7002, Final Paper May 6, 2006.

[5.] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[6.] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[7.] Davis, R., "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

[8.] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.
[9.] Pratap Chnadra Mandal "Superiority of Blowfish Algorithm," International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.
[10.] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[11.] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.

**M. Surya Prakash** is a student of b.tech fourth year in Computer science from Siddhartha Institute of Engineering and Technology. His subjects of interest are Big Data and Database security.

**B. Mahender Reddy, M.Tech,** working as Asst. Prof at CSE Dept in Siddhartha Institute of Engineering and Technology, Ibrahimpatnam. His area of interest is Database Management System, Computer programming, OOPS Through Java, Advanced Data Structures and Algorithms and Data Science

**S.Rajesh,** M.Tech, working as Asst. Prof at CSE Dept in Siddhartha Institute of Engineering and Technology, Ibrahimpatnam. His area of interest is Database Management System, Computer programming, Cloud Computing and Data Science