Secured E-Mail

Ms. Sanskruti Jayprakash Joshi
Department of Computer Science & Engineering
Walchand Institute of Technology, Solapur, India

Abstract— The main aim of the project is to increase the security of the mails that user sends. In the existing system, the mails that user sends to other users can be forwarded further and the data that has been sent has no security associated with it. In this new system that is "SECURED MAIL", the proposed system associates security to the data that has been sent. Users need to create an account to get the benefit of the security of the data. The data sent by the user has a password associated with it. The other user can unlock the data only by inserting the password that was assigned by the sender. Receiver can only access the data with the password but he cannot download that data in his/her PCs, laptops, mobiles etc. Every other receiver needs newly generated password from the sender to access the data thus providing security and enhancement to the existing system.

Key words: CP-ABE, 2PC Protocol, Dynamic Key Generation Algorithm, Data Security, Email Security

I. INTRODUCTION

Nowadays email has become more adequate in industry so the importance of its security has also become significant. Security contains management of email storage and data recovery. When data is large then managing and storing it takes a lot of time that will impact the user. Email security has become crucial in organizations, businesses and every other field. Email security refers to protection from various attacks. The architecture of network is major part while securing an email. Many organizations use firewall to prevent these attacks. To understand the email security research, it is necessary to understand its background. Simple Mail Transport Protocol (SMTP) was designed for a smaller community of users. Several technology and policy changes were made to SMTP server to make email secure. It does not contain incompatibility between older and newer systems. Security in information technology is defined as to protect information against unauthorized revelation as well as unauthorized modification. User needs to take care about possibility of malicious and fraudulent attacks by hackers as well as impact of viruses and denial-of-services attack. Some of approaches that is useful for security of your system includes: Authentication, Access Control ,Encryption ,Firewall ,Intrusion detection and Anti-virus software. For E-mail security, SMTP is the first protocol which is used for security purpose. In Email messaging, security contains privacy, Sender authentication, Message integrity, Non-repudiation and Consistency. But it contains some limitations. Thus, from the last few years the need for email security has increased. As more and more users connect to the internet it attracts a lot of criminals. Billions of transactions happen every hour over the internet, this need to be protected at all costs.

II. LITERATURE SURVEY

In ref. [10], they have used the algorithm of encoding technique to secure the medical documents such as patient details. But From a security point of view, even if it had worked in practice, this would have been a very weak encryption algorithm for two reasons. First, there is no secret key. Therefore, it is not a true encryption scheme, but an encoding scheme. Anyone who knows operation method is unknown to an attacker or even if a secret key is introduced, the algorithm is a simple substitution cipher, which means that the same plain character will always be encrypted into the same cipher character under the same key.

In ref. [11], Block-Based Algorithm there are various technique used as follows Blowfish algorithm has best performance for the small data size so it is not applicable for large data. It resulted in higher correlation and lower entropy .So they proposed new algorithm. In that original data was divided into blocks, which were rearranged into a transformed data using a transformation algorithm and then the transformed data was encrypted using the Blowfish algorithm but for rearranging the data it takes lot of time than the actual encryption of data. The algorithm was commercially available, the ciphered data that resulted from applying the proposed algorithm on different block sizes of the original data using the proposed algorithm. Combined approach gives better performance compared to single algorithm implementation.

In ref. [12], Steganography is the art of covering secret and confidential information within a carrier which could be any data file, image file, video file or audio file. It was a technique which provides invisible communication since a data file which had the secret information embedded within it is delivered to the receiver instead of the secret information itself. It is protecting information by transforming into unreadable format called cipher text. Only those who possess a secret key can decrypt or decode the message into plain text.

In ref. [13], the Particle Swarm Optimization (PSO) for data authentication and tamper proofing is discussed. This scheme provide solutions to the issues such as robustness, security and tamper detection with precise localization. The features were extracted in Daubechies4 wavelet transform domain with help of PSO to generate the data hash. This scheme was moderately robust against attacks and to detect and locate the tampered areas in the data. This system uses Hash based techniques. Hash based techniques are different from the watermark based techniques in authentication. The advantages of hash based techniques are no distortion is introduced in the image to be authenticated and content hash generated in frequency domain which has more robust to geometric distortions compared to their spatial domain counterparts.

In ref. [14], the techniques used are virtual private network (VPN), data encryption; and data embedding is being used for additional data protection in other fields of applications like financing, banking, and reservation systems. However, these techniques have not been systematically applied to medical purpose partly because of the lack of urgency until the recent HIPAA proposed requirements in patient data security.

In ref. [3], one policy is cipher text Policy Attribute Based Encryption (CP_ABE) for example primary health care center scenario for a patient attribute. The major drawback is key escrow problem. Advantage is the data owner can access the patient details easily. In key generation center decryption is carried out by private keys. In data sharing scenarios, attribute based methods are not suitable, since system can share only to the designated users.

Cloud over data privacy is achieved by using encryption techniques. The security of network is consisting of different approaches and techniques to achieve the data cryptographic security. The most commonly used method in recent time is Attribute-based encryption (ABE). If a user sends data through the access request to the cloud, the cloud will return to the same cipher text data user, a user to decrypt the data using your private key. But this would lead to some problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to complete this.(2) a lot of storage overhead would be spent because of the same plaintext with different public keys. In order to overcome these limitations an attribute-based encryption (ABE) technique is used.

III. Proposed Solution

Every system has certain drawbacks and Gmail, Yahoo, etc. are no such exception. In our system the data cannot be forwarded or downloaded without the permission of the authorized user.

In this system the third party member cannot manipulate the data and thus, the integrity, confidentiality and authentication of the data is maintained in its original format.

A. Advantages:

1) The data cannot be forwarded without the permission of the authorized user. The authorized user sends the key to access the data only then the data can be read.
2) The data cannot be downloaded.
3) The data cannot be printed using print screen.
4) The data cannot be copied by using right click.
5) Security and authentication of the data is maintained.

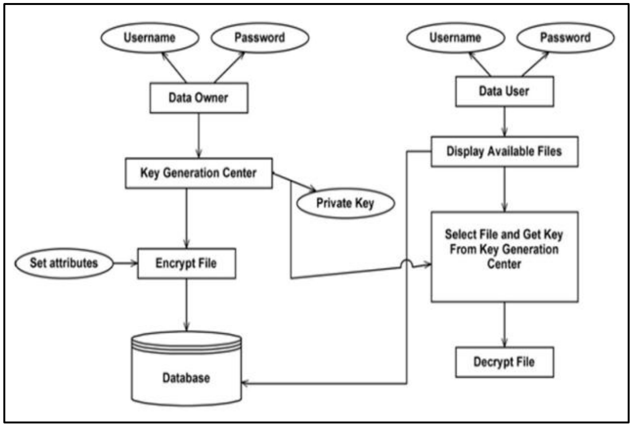


Fig. 1: Work flow

The working depends mainly on the two components which are as follows:

1) Data Owner

– Data owner enters the username and password then selects the data to be uploaded.
– The data will be encrypted and a unique key will be generated at Key generation center. Then the data will be stored on database with the key

2) Data User

– The User will select the data and requests the owner for the key.
– After that user will enter the key and the data will be decrypted to the original form.

3) Steps performed by Data Owner

– Owner Register.
– Owner Login.
– Select data to upload.
– Encrypted image will be converted to text file and is stored in database.
– System will generate unique key for the data using Key generation algorithm.
– Owner will approve the request.
– The generated key will be given to the user requesting the key through mail.
– Owner Logout
– Steps performed by Data User
– User register.
– User Login.
– Request for data to Owner.
– User will get key from Owner.
– User will enter the key.
– The data will be decrypted and then will be read.
– User Logout.

IV. Result

A. Registration page:

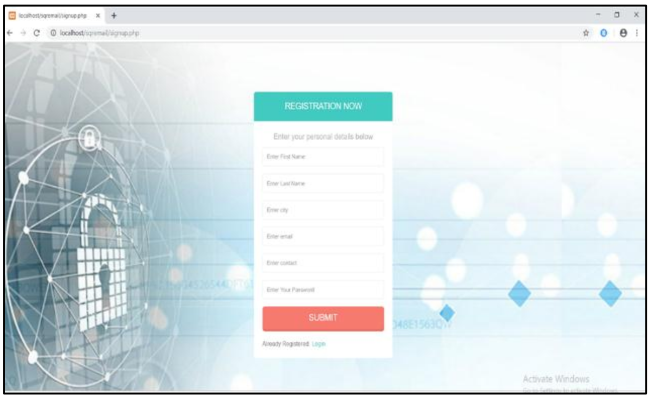


Fig. 2: User registration page

B. Sign-in page:

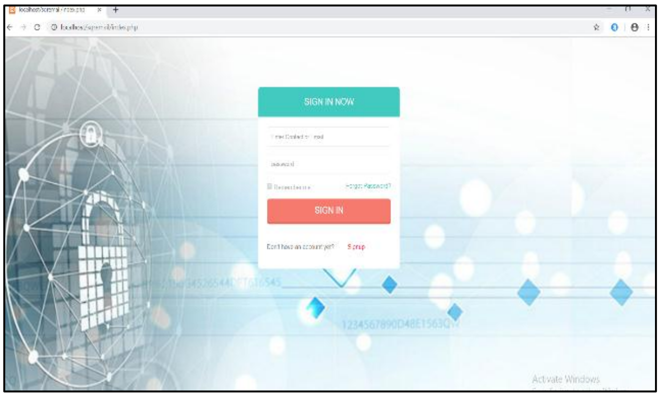
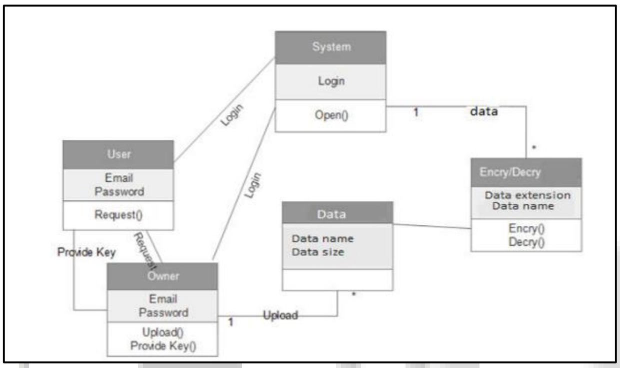


Fig. 3: User sign-in page

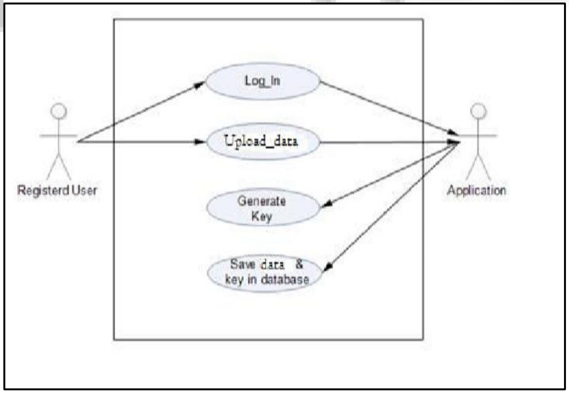
V. Data Flow Diagrams and Sequential UML Diagrams

A. Data flow diagram:

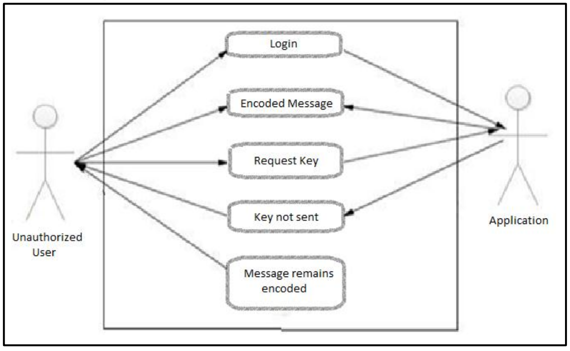


B. Sequential UML diagrams:

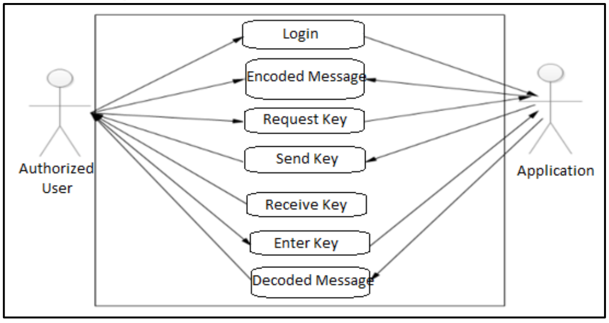
1) Use case for registered user:



2) Use case for unauthorized user:



3) Use case for authorized user:



VI. Future Scope

The system would be beneficial for organizations where confidential data needs to be exchanged. Organizations using the system would be able to maintain integrity and authentication of the data and keep it more secured. The current system cannot receive or send emails from other mailing services. Thus future work would include expanding proposed system by providing connectivity to other mailing services and make it more user-friendly.

VII. Conclusion

From the last few years the need of email security has also increased. Internet has become an important part of our daily life and along with that we deal with emails in our day to day life. As more and more users connect to the internet it attracts a lot of criminals. Today, everything is connected to internet from simple shopping to confidential banking transactions so there is need of network security. Billions of dollars of transactions happens every hour over the internet, this data requires complete integrity and security.

Even a trivial malicious attack in a network can have an enormous impact on the system. If company's records are leaked, it can put the user's data such as their banking details and credit card information at risk. Numerous software's such as intrusion detection have been used which prevents these attacks. But most of the times it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following many simple methods as outlined in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them.

References

[1] J.-M. Zhu and J.-F. Ma, "Improving Security and Efficiency in Attribute Based Data Sharing," IEEE Transactions on knowledge and data engineering, vol. 25, no. 10, October 2013

[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp.Security and Privacy, pp. 321-334, 2007

[5] X. Liang, Z. Cao, H. Lin, and D. Xing, “Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption,” Proc. Int’l Symp.Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009

[6] M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009

[7] S.S.M. Chow, “Removing Escrow from Identity-Based Encryption,” Proc. Int’l Conf. Practice and Theory in Public Key Cryptography (PKC ’09), pp. 256-276, 2009

[8] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryption with Efficient Revocation,” Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded Ciphertext Policy Attribute-Based Encryption,” Proc. Int’l Colloquium Automata, Languages and Programming (ICALP), pp. 579-591, 2008

IJSRD