Enchancing Email Security– End-to- End Encryption

Ms. Sayali Gaikwad[1], Dr. R.R. Dube[2]

[1,2]Department of Electronics Engineering Walchand Institute of Technology Solapur, India

Abstract—Nowadays, the majority of consumers and businesses utilize email for a variety of purposes, including user information communication. One crucial network application is the email client. It is significant when it is used by the business, medical, and educational groups for the transmission of crucial information like business data, patient medical records, and so forth. Data and messages can be easily transmitted between senders and receivers across internal networks or the Internet, enabling messages to be received, forwarded, saved, and broadcast to recipients. Electronic mail is accessible through a wide range of suitable software clients, as well as through a web browser, and is also widely used for personal usage. Electronic mail must be defended on both the sending and receiving sides because of its widespread use, making it both a great target and the main attack vector.

Security processing is added to a corporate email implementation's second service model. In a completely outsourced model, the service provider is in charge of keeping track of any risks that use email as a channel (such as spam, phishing, virus propagation, etc.), as well as of providing an email user interface (UI). In the enterprise augmentation concept, extra cloud-based services and functionalists are added to an existing on-premise email implementation. This paper delves into identity federation and data loss prevention, as well as best practices for analyzing, designing, installing, and deploying cloud-based email security services. Target Market Two viewpoints are taken into consideration when discussing email security services: those who offer these services and those who use them or buy them. Both parties must be aware of and make plans for essential service features in order to address threats to email security.

Keywords— E-mail security, Encryption, Key generation, Data storage.

I. INTRODUCTION

Email security refers to a variety of methods for protecting confidential information in email correspondence and accounts from unwanted access, theft, or compromise. Malware, spam, and phishing attacks are frequently disseminated by email. These attacks use misleading messages to persuade users to give personal information, open attachments, or click on hyperlinks that download malware onto the victim's computer. For hackers attempting to penetrate an enterprise network and access sensitive data, email is another popular entry point. Both personal and business email accounts require email security, and companies should take a variety of steps to strengthen email security.

The ease and speed with which email may be sent, regardless of geographic distance, is perhaps its primary benefit. An email has open access to the systems it passes through, just like a postcard does. Information can be easily intercepted, copied, or sought after by anyone. Emails are used to share sensitive data, including bank statements, trade secrets, and even information that is considered to be a national secret. Email content is becoming more precious and significant than ever, and this has many people worried about its security. Current email encryption systems need costly operations and hard key management, which is the main deterrent for utilizing encryption in email exchanges. Therefore, there is a huge demand for research on straightforward, highly secure, and effective email systems.

There are numerous methods. Email security refers to safeguarding confidential information in email correspondence as well as account security from theft, loss, or compromise. Email is a well-known channel for the dissemination of malware, spam, and phishing attacks in an enterprise network and the breach of valuable company data. These attacks use deceptive messages to lure recipients into disclosing sensitive information, opening attachments, or clicking on hyperlinks that install malware on the victim's device. Attackers who want to take control of both personal and commercial email accounts frequently enter through email, so businesses should take a number of steps to strengthen email security.

II. RELATED WORK

Steganography is the practice of hiding sensitive information within a carrier, such as an image, video, or audio file. The secret information was placed in a picture file that was sent to the recipient instead of the secret information itself, making it an invisible communication method. It is a method of information security that involves converting data into cipher text, an unintelligible format. Only those who have access to the secret key can convert the message from plain text into encryption.[1]

The algorithm of encoding approach was utilized the research to secure the image documents. However, even if it had actually worked, from a security perspective, this encryption scheme would have been exceedingly unreliable for two reasons. First off, there isn't a hidden key. As a result, it is an encoding system rather than a genuine encryption one. Anyone who is familiar with how it works can retrieve the original content with ease. Second, the technique is a basic substitution cipher, which implies that the same plain character will always be encrypted into the same cipher character using the same key, even if the operation method is unknown to an attacker or even if a secret key is inserted.[2]

Various techniques are employed in Block-Based Algorithm, including the ones listed below. Large images cannot use the blowfish algorithm. since it performs best for the lowest image block size. Higher correlation and lower entropy were the outcomes. They then suggested a new algorithm. The original image was divided into blocks, which were then rearranged to create a transformed image using a transformation algorithm. The modified image was then encrypted using the Blowfish technique, but the process of rearranging the images takes far longer than the encryption process itself. They used the commercially available algorithms on the ciphered image that was produced as a result of using the suggested algorithm along with the other algorithms, and the performance was better than when the other algorithms were used alone.[3]

Particle swarm optimization (PSO) for picture authentication and tamper-proofing was explored. For reasons including durability, security, and accurate localisation of tampering The issues are addressed by this plan. PSO was used to extract the features in the domain of the Daubechies4 wavelet transform in order to produce the picture hash. This method could detect and pinpoint the tampered areas in an image and was moderately resistant to attacks. They employed hash-based approaches in this. In picture authentication, hash-based approaches are different from watermark-based techniques. In order to create a compact representation that can be used for authentication, an image hashing algorithm extracts a number of features from the image. The benefits of hash-based techniques include the fact that no distortion is added to the image being verified and that the content hash is formed in the frequency domain, which is more resistant to geometric distortions than its counterparts in the spatial domain. [4]

One policy cipher text Policy Attribute Based Encryption (CPfABE). As an illustration, consider the case of a primary healthcare center and a patient attribute. Key escrow problem is the main negative. Advantage: Patient information can be simply accessed by the data owner. Private keys are used at the key generation center to perform decryption. Attribute-based techniques are not well suited for data sharing scenarios because we can only share with designated users.[5]

The privacy of cloud-based data is attained through the use of encryption methods. To accomplish data cryptographic security, a variety of strategies and methods are used in network security. presently is The approach that is most frequently employed is attribute-based encryption (ABE). If a user submits an access request to the cloud, the cloud will return the identical ciphertext data to the user, who must use your private key to decrypt the data. This could result in the following issues: (1) In order to encrypt data, the data owner must get the data user's public key; (2) because the same plaintext may be used with various public keys, a significant amount of storage overhead may be incurred. A BE, or attribute-based encryption, was developed to get around these restrictions and other issues.[6]

III. NEED FOR EMAIL SECURITY

Due to the ubiquity of email as an attack vector, it is imperative that businesses and individuals take precautions to protect their email accounts against conventional attacks as well as illegal attempts to access accounts or messages. Email- borne malware has the potential to be very damaging. Phishing emails addressed to employees frequently include links to malicious websites or attachments that are disguised to look like authentic papers. All it takes for accounts or devices to be compromised is opening an email attachment or clicking on a link in an email. Phishing emails can also be used to fool users into giving private image information, frequently by pretending to be a reliable company or a contact they know and trust. Phishing attacks against corporations frequently target divisions like accounts payable or human resources that deal with sensitive personal or financial information. In addition to impersonating known vendors or company executives, attackers will try to instill a sense of urgency in phishing emails to increase their chances of success. Phishing emails aimed at stealing information typically will ask recipients to confirm their login information, images passwords, social security number, bank account numbers, and even credit card information. Some even link to counterfeit websites that look exactly like that of a reputable vendor or business partner to trick victims into entering account or financial information.

IV. SYSTEM DESIGN

The overall technique is as follows that the data owner enters their account and password, then selects photographs to upload or data to send to the specific recipient. This information will be encrypted using a special key that is generated at the key generation center. The key-protected database will hold the data. User will choose the data and ask the owner for the key so that the receiver can access the data. The data will be decrypted to its original form when that user enters the key. Resulting in the creation of a secure environment for the data transfer.

There are several ways to secure email accounts, and for businesses, it usually involves a two-pronged strategy that includes staff education and thorough security standards. Among the best email security techniques are: Encourage staff to participate in continuing security training about the dangers of email phishing and how to prevent becoming a victim of one. Employees must utilize QR-encrypted passwords, and password updates must be required on a regular basis. Protect email attachments and email content by using email encryption. If your business permits employees to access corporate email on personal devices, then you should implement BYOD security best practices. Make sure webmail programs can employ encryption and safe logins. Utilize scanners and other tools to filter emails containing malware or other harmful files and check communications before they reach your end users. Use a data protection system to identify sensitive information and guard against email loss.

IV.I SETUP PHASES

A. Registration Phase:

Initial phase involves user entering username, password, and mobile number. They are then prompted to select the picture matrix after selecting the security level. The quantity of messages depends on the 2^n when the security level is set to be 2^n. The user must next input their messages in the message box, choose how they want those communications to be converted, and have those converted messages shown in the registration part below as QR pictures.

B. Login Phase:

Depending on the security level matrix of the presented QR pictures, the user enters their user ID and password during the login phase. The user registers the appropriate encoded image during the registration process.

C. Verification Phase:

The system compares the data entered with the data entered at registration time, i.e., the system checks the level-by-level selection of the image, and if any level is unsuccessful, the system may abruptly terminate the user's session without prior notice.

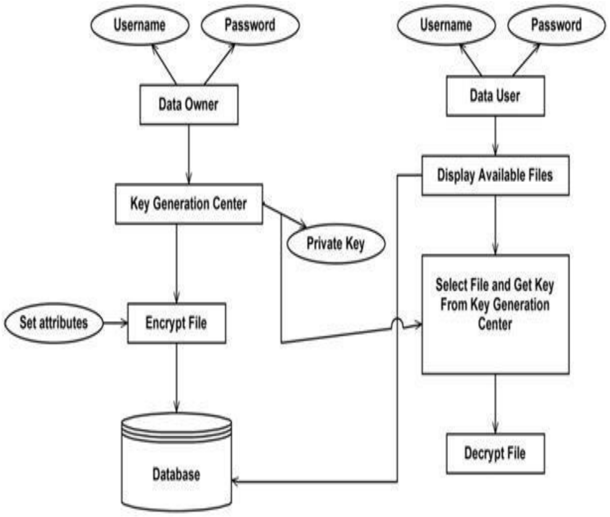
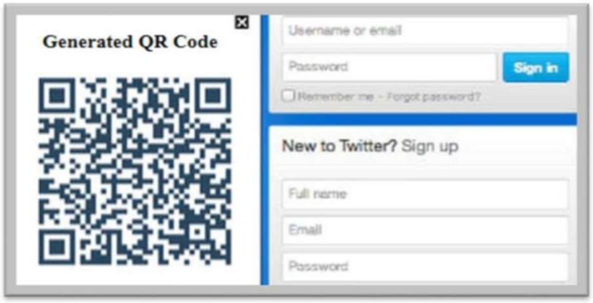


Fig. 4.1

D. Key generation center:

The primary authority in charge of generating public and private parameters. It is in responsible of granting, cancelling, and modifying attribute keys for users. Individual users can be granted varying levels of access based on their attributes. It is assumed to be truthful but curious. That is, it will carry out the tasks allocated to it in the system honestly; nonetheless, it would prefer to learn as much as possible about encrypted content. As a result, even if it is honest, it should be barred from accessing the plaintext for which the encrypted data was created.



Generated QR Code

Username or email

Password

Sign in

□ Remember me · Forgot password?

New to Twitter? Sign up

Full name

Email

Password

Fig.4.2

E. Data-storing center:

It is an entity that offers a data-sharing service. It is in charge of controlling external user access to data storage and offering corresponding content services.

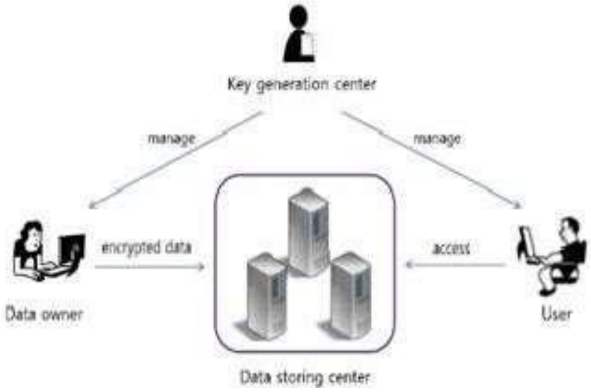


Fig. 4.3

IV.II ENCRYPTING THE IMAGE

A. Data Owner

The client is the one who owns the data and wants to upload it to the external data storage facility for cost or ease-saving purposes. A data owner is responsible for creating (attribute-based) access policies and enforcing them on its own data by encrypting it before distributing it.

B. User

It is an entity that wishes to gain access to the data. If a user has a set of attributes that fulfill the encrypted data's access policy and is not revoked in any of the valid attribute groups, he will be able to decrypt the ciphertext and acquire the data. Because both key managers, the KGC and the data storage center, are semi-trusted, they should be discouraged from gaining access to the plaintext of the material to be shared; yet, they should still be allowed to give secret keys to users. To meet this rather conflicting condition, the two parties employ the mathematical 2PCprotocol with their own master secret keys, and issue independent key components to users during the key issuance phase. The 2PC protocol prevents them from knowing each other's master secrets, preventing them from individually generating the entire set of user secret keys.

IV.III DATA FLOW DIAGRAM

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system that models the process characteristics of the system. A DFD is frequently used as a first step to produce an overview of the system that may subsequently be elaborated. A data flow diagram (DFD) depicts the type of information that will be input to and output from the system, where the data will come from and go to, and where the data will be kept. It does not display information about the timing of processes or whether they will run in succession or in parallel.

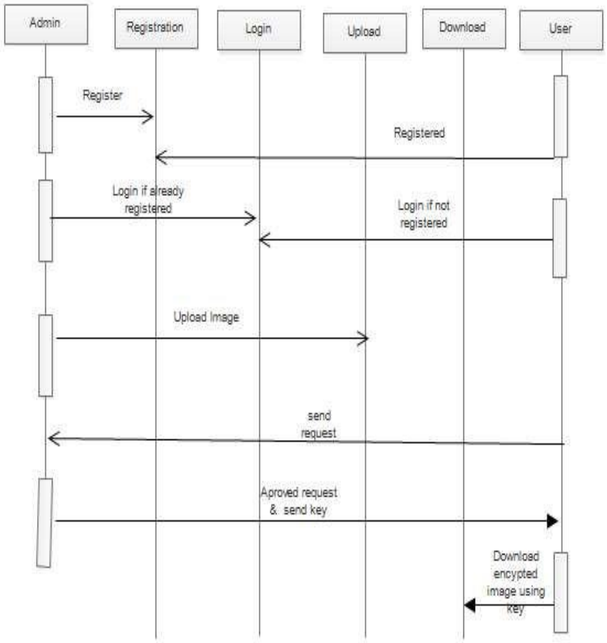


Fig.4.4

IV.IVACTIVITY DIAGRAM

Activity diagram depicts that the user must first register and login, and then, if the user is an administrator, it will proceed to the User1 flow, and if the user is a simple user, it will go to the User2 flow, and eventually logout.

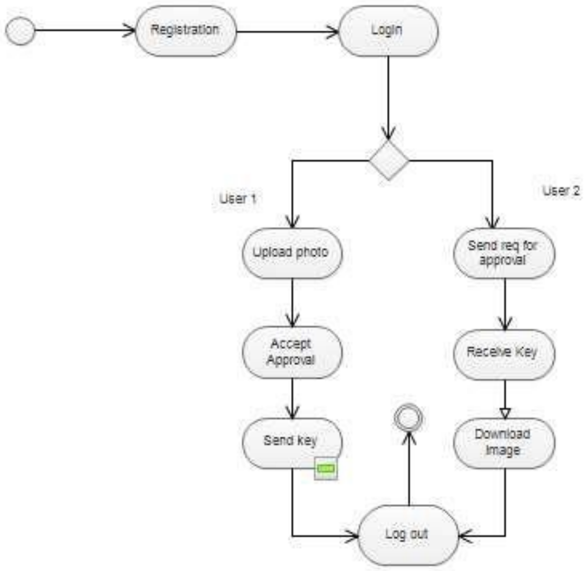


Fig. 4.5

V. CONCLUSION

The suggested system addresses the security flaws in the currently used mail servers by enhancing the security of emails, particularly those carrying sensitive information. Due to the use of only one level of security, a login-password scheme, hacking has grown to be one of the biggest risks to today's email systems. The created program, which uses three layers of authentication, gives essential emails sent over the Internet increased security and guarantees that users won't have to worry about their messages being intercepted. It creates a safe system to guarantee that the crucial information is neither leaked or used inappropriately, making it the perfect mailing system. It enhances plaintext email with privacy, authentication, message integrity, and non-repudiation.

REFERENCE

[1] What Email servers can tell Johnny: An Empirical Study of Provider-to-Provider Email Security. July 24, 2020

[2] A Survey of Email Service; Attacks, Security Methods and Protocols. International Journal of Computer Applications (0975 – 8887) Volume 162 – No 11, March 2017

[3] A Solution for Secure Certified Electronic Mail Using Blockchain as a Secure Message Board. March 2019

[4] Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. April 23, 2018.

[5] Enchancement of email security. International Journal of Scientific & Engineering Research, Volume 8, Issue 1, January-2017

[6] K. Kuppusamy and K. Thamodaran "PSO based optimized security scheme for image authentication and tamper proofing "

[7] Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan "Data Security Using Image Steganography And Weighing Its Techniques"

[8] Mohammad Ali Bani Younes and Arnan Jantan "Image Encryption Using Block-Based Transformation Algorithm

[9] Suresh Kumar Balakrishnan and V. P. Jagathy Raj, "Practical Implementation of a Secure Email System Using Certi_cateless Cryptography and Domain Name System", International Journal of Network Security, Vol.18, No.1, PP.99-107, Jan. 2016.

[10] An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 3, March 2013

[11] 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

[12] 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.

[13] 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