iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59921

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Enhancing Email Security - End to End Encryption

Ms. Sayali Gaikwad[1], Dr. R. R. Dube[2]
Department of Electronics Engineering, Solapur University

Abstract: ***Nowadays, most of people and organizations use the e-mail for different needs to exchange information between users. E-mail application is an important network application. It is significant when business1, health and educational communities use it for exchange of critical information such as business information, health patient record and so on. over the Internet or internal networks, It allows data and messages to be transferred easily between senders and receivers allowing messages to be received, responded to, stored, forwarded and broadcast among recipients. These extensive capabilities have caused the email to be widely adopted as the official communications method for many organizations. Also common for personal use, electronic mail is available through a diverse number of compatible software clients, and also via web-browser.***
An existing enterprise email implementation second service model adds security processing. The service provider is responsible for monitoring all threats using email as a channel , and for providing an email user interface (UI) In the enterprise augmentation model, an existing on-premise email deployment is augmented by additional cloud-based services and functionalist. This paper explores identity federation and data loss prevention and describing best practices for evaluating, developing, installing and using cloud-based email security services.1.1Intended Audience Email security services are viewed from two perspectives: the providers of these services and the consumers or purchasers of email security services. key service features is needed for both sides to be aware of and plan for and how these features are used to tackle threats to email security.
Keywords: image security, Mail Security

I. INTRODUCTION

In the field of information security, E-mail security becomes a critical issue for the research community. In order to enhance e-mail security. Focusing keeping the exchange of data via e-mail there are several solutions and standards have been fashioned according to the recent security requirements of the existing enhancements in a confident and integral way. This paper will propose various e-mail security solutions. We introduce techniques used to solve and enhance the security of e-mail systems.
Email security describes for accounts secure against unauthorized access, loss, or compromise. Using deceptive messages to entice recipients to divulge sensitive information, click on hyperlinks that install malware on the victim's device or open attachments, email is a popular medium for the spread of malware, spam, and phishing attacks, In an enterprise network and breach valuable company data. Email is also a common entry vector for attackers looking to gain a foothold for both individual and business email accounts, and there are multiple measures organizations should take to enhance email security. The Need For Email Security Via email messages, Malware can be sent be quite destructive. Legitimate documents or include hyperlinks in attachments that lead to websites that serve malware Phishing emails sent to people often contain malware. Often by posing as a legitimate business or trusted contacts Opening an email attachment or clicking on a link in an email can be all that it takes for accounts or devices to become compromised. Phishing emails used to trick recipients into sharing sensitive image information, Often target departments that handle sensitive personal or financial information which Phishing attacks against businesses, such as accounts payable or human resources. Phishing emails focus on stealing information will ask recipients to confirm their social security number, login information, bank account numbers, image passwords, and even credit card information.

II. LITERATURE REVIEW

A. Security Point Of View

In ref[10] paper they were used the algorithm of encoding technique to secure the image documents. 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 can easily recover the original text who knows its operation method.

B. Block-Based Algorithm

In[11] Block-Based Algorithm there are various technique used as follows Blowfish algorithm has best performance for the smallest image block size so it is not applicable for large images. It resulted in higher correlation and lower entropy.

©IJRASET: All Rights are Reserved

So, using a transformation algorithm, original image was divided into blocks, which were rearranged into a transformed image and then the transformed image was encrypted using the Blowfish algorithm but for rearranging the images it takes lot of time than the actual encryption of images. The algorithms were commercially available, so they applied them on the ciphered image that resulted from applying the proposed algorithm along with the other algorithms resulted in a better performance.

C. Steganography

In ref[12] Steganography is the art of covering confidential and secret information within a path which could be an audio file, video file or image file. It was a technique that provides an image file which had the secret information embedded within it is delivered to the receiver. The ciphertext is protecting information by transforming it into an unreadable format. so for those users who possess a secret key can decrypt or decode the message into plain text.

D. Particle swarm optimization (PSO)

In ref[13] they discussed the Particle swarm optimization (PSO) for image authentication and tamper-proofing. For such as robustness, security and tamper detection with precise localization This scheme provides solutions to the issues. In the Daubechies4 wavelet transform domain with the help of PSO the features were extracted to generate the image hash. This scheme was moderately robust against attacks and to detect and locate the tampered areas in an image. In this, they were used Hash-based techniques. Hash-based techniques have differed from the watermark based techniques in image authentication. An image hashing techniques extract a set of features from the image used for authentication. The advantages of hash-based techniques are no distortion is introduced in the image to be authenticated and content hash generated in the frequency domain which has more robust to geometric distortions.

E. Virtual Private Network (VPN)

In [14] They used the techniques 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. To overcome this drawback, the picture archiving and communications system (PACS) is an integrated management system for archiving and distributing medical image data was introduced. Usually over the internal hospital network Communication of medical images in a PACS environment is that is protected by a firewall from outside intruders.

F. Cipher Text Policy Attribute Based Encryption CPfABE

In [3] one policy is cipher text Policy Attribute Based Encryption CPfABE.for example primary health care center scenario for a patient attribute. The major drawback is key escrow problem. In KGC decryption carried out by private keys. Advantage is to data owner can access easily patient details.

G. Summery

Cloud over data privacy is achieved by using encryption techniques. The security of the network is consisting of different approaches and techniques to achieve data cryptographic security. Recent time is Attribute-based encryption (ABE) is the most commonly used method. If a user sends through the access request to the cloud, the cloud will return to the same ciphertext data user, a user to decrypt the data using your private key. This manner may lead some problems: (1) t should encrypt data, the data owner needs to obtain the data user's public key to complete this; (2) a lot of storage overhead may spkend because of the same plaintext with different public keys In order to overcome these limitations, and so forth, an attribute-based encryption (ABE).

III. METHODOLOGY

The block diagram explains

1) Data owner enter their username and password then select images to upload
2) This image will be encrypted and a unique key will be generated at Key generation center.
3) The images will be stored on database with the key.
4) User will select image and request for the key to owner. After that user will enter the key and the image will get decrypt to the original form.

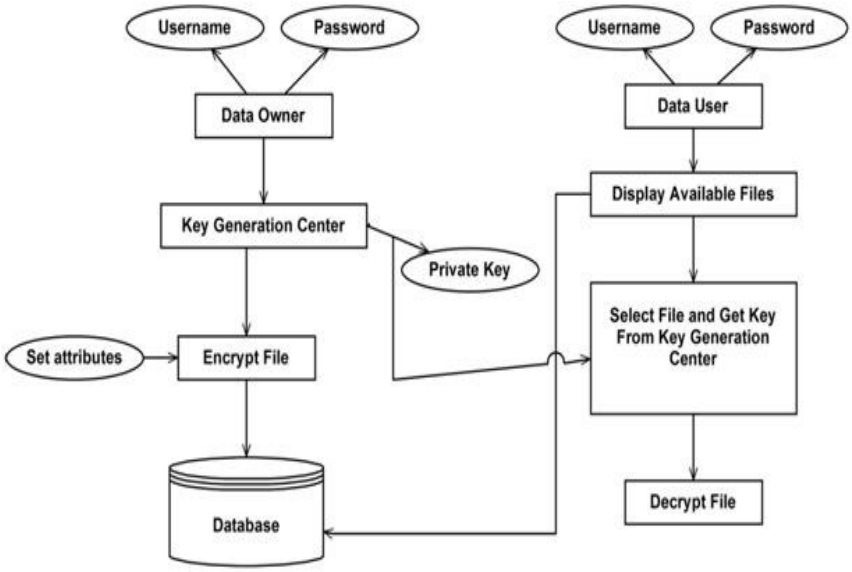


Fig. Proposed system architecture

IV. CONCLUSIONS

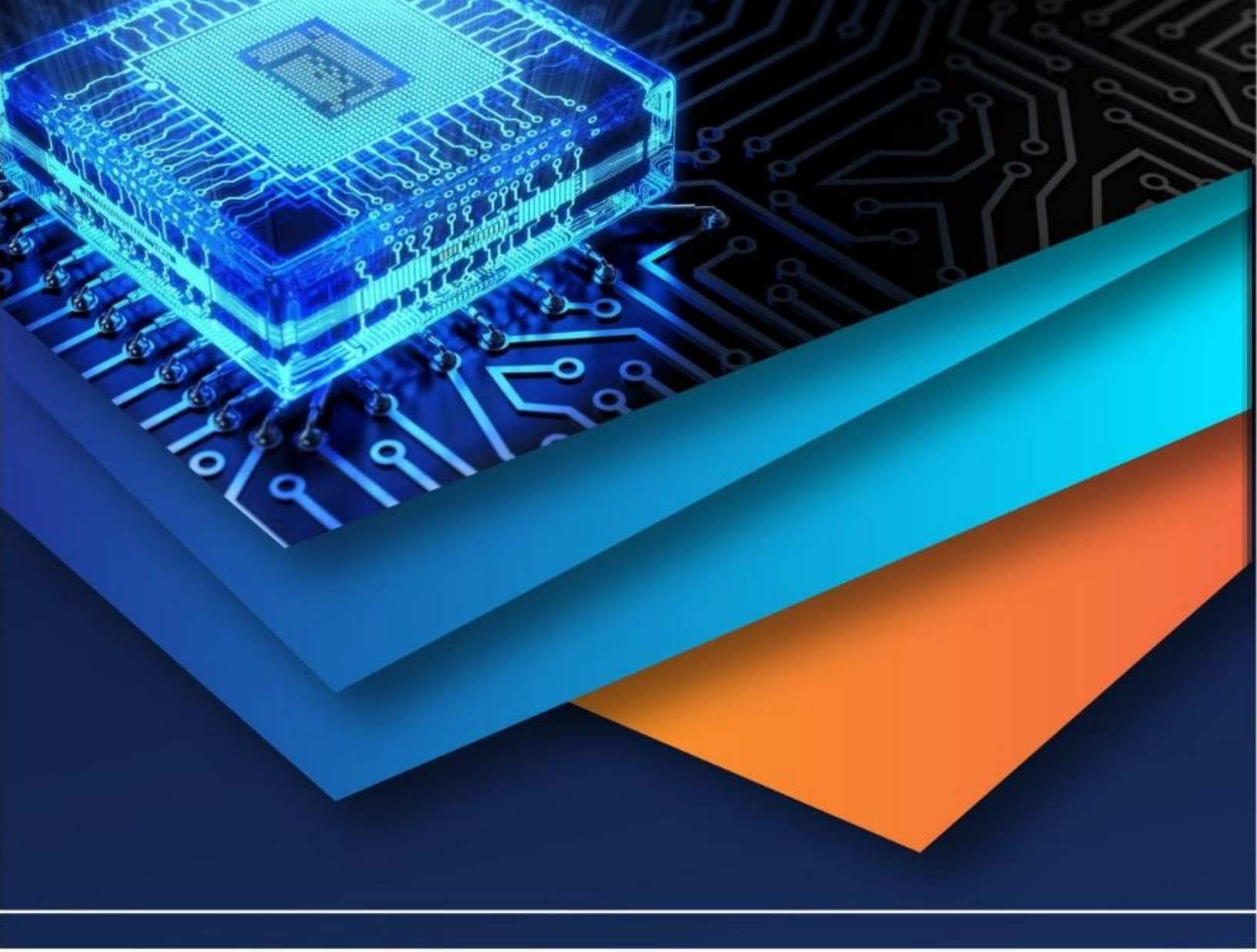
The proposed system overcomes the drawbacks found in the present existing mail servers regarding security by providing better security for the mails especially containing critical information. Hacking has become one of the greatest threats faced in today's mailing systems due to the usage of only one 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.

V. FUTURE SCOPE

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.

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.
[10] Gonzalo Alvarez, Shujun Lib, Luis Hernandez "Analysis of security problems in a medical image encryption system"
[11] Mohammad Ali Bani Younes and Arnan Jantan "Image Encryption Using Block-Based Transformation Algorithm "
[12] Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan "Data Security Using Image Steganography And Weighing Its Techniques"
[13] K. Kuppusamy and K. Thamodaran "PSO based optimized security scheme for image authentication and tamper proofing ".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)