Securing Enterprise Emails in Cloud Platform

[1]Nabeena Ameen, [2]Sumaiya Mubasshara.H, [3]Fiza Hussain.M
[1,2,3] Department of Information Technology,
[1,2,3] B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur, Chennai – 600048
[1]nabeena@crescent.education, [2]sumaiya271331@gmail.com, [3]fiza16hussain@gmail.com.

ArticleInfo
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202202008
Received 28 December 2021; Revised form 20 February 2022; Accepted 05 March 2022.
Available online 05 April 2022.

Abstract – Cloud-based email is one of the services offered by cloud computing, and the number of users continues to grow year after year. Because of its working environment, cloud computing raises concerns about security and privacy. User authentication in cloud computing is now predicated on the user's credentials, which are typically username and password. User authentication in cloud computing is currently predicated on the credentials possessed by the user, which are primarily username and password. With the growing usage of cloud emails and numerous allegations of large-scale email leakage occurrences, a security attribute known as forward secrecy has become desirable and necessary for both users and cloud email service providers to strengthen the security of their communications. However, due to the failure of email systems to meet both security and practicality requirements at the same time. A fine-grained revocation capacity is available to an email user. A security key will be provided by the user to prevent hacking of such email addresses. The MAES(Modified Advanced Encryption Standard) algorithm encrypts files and a user's email ID to safeguard their data from a third party or hackers to address this issue more efficiently. This proposed hybrid security method secures the content of emails before they are sent through email using an Advanced Cipher Technique (ACT). The study suggests employing substitution and permutation to secure email content, with the fronts offered by email systems acting as keys.

Keywords – User Authentication, MAES, Security Attribute, Cloud, Email.

I. INTRODUCTION

Email has long been one of the most popular ways for individuals and businesses to send and receive data and information. Furthermore, the rapid adoption and commercialization of cloud computing has also aided small businesses and startups in deploying their own cloud email systems, [1] which are considerably more scalable and cost effective than traditional solutions. This increases the number of people who use email.

Cloud email security solutions are secure email platforms that help customers from falling for phishing scams that fool them into handing over sensitive information. The platforms, which are hosted by a cloud email security vendor, also ensure that emails that contain links to harmful websites or that initiate malware downloads are stopped before they reach the end user. Cloud email security solutions are used by businesses to prevent data loss and the release of privileges or credentials, as well as to boost productivity. [2] By blocking malware and other web-based threats, you may improve endpoint security.

II. PROBLEM DEFINITION

When migrating email services to the cloud, most businesses will notice some significant differences in terms of security. First, depending on which provider the firm picks and how it provides[3, 4] an email service, there's a potential that visibility of activities will be decreased. In most circumstances, real-time visibility is harmed, and in certain cases it is substantially harmed.

Enterprise security teams rely on email platform logs and alerts as a main signal of anomalous behaviour and threats, and receiving fewer logs, [5] logs with less detail, or logs after the fact may jeopardise many security teams' overall security monitoring and response efforts.

III. METHODOLOGIES

Proposed System

Concept: The purpose of authentication procedures is to protect resource access. After receiving their registration details, service providers want to give authorization services to users or customers, [6] depending on their preferences.

Technique: Modified AES algorithm

Advantage: It follows a common protocol for sharing data in order to communicate.

IV. ARCHITECTURE DIAGRAM

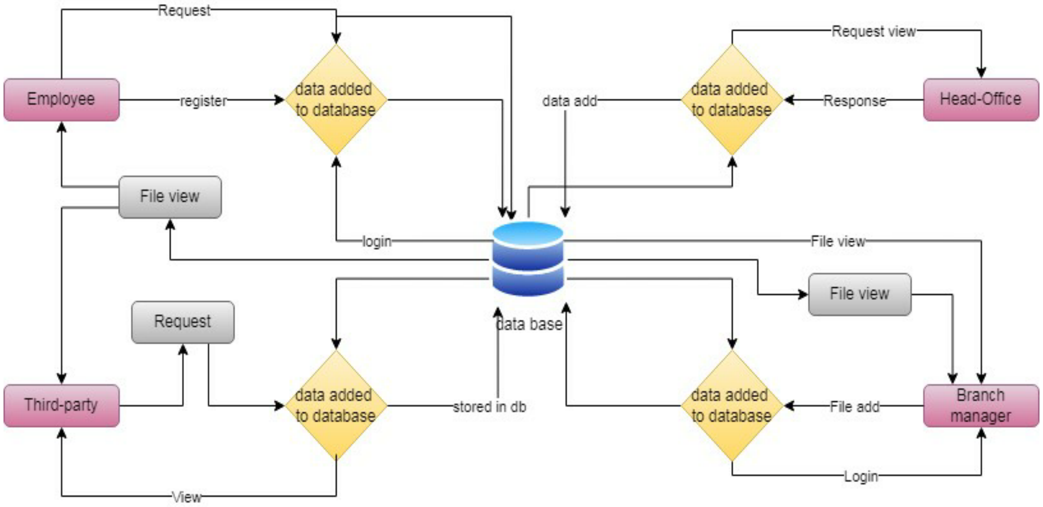

Fig 1. System Architecture

Fig1. The system's architect builds the system's basic structure; we sugge st the Hash code Solomon technique, and we can store a tiny portion of data locally to ensure privacy. [7,8] Furthermore, this approach can compute the distribution proportion stored in the cloud and local computer, respectively, using computational intelligence. The practicality of our method has been proven by theoretical safety analysis and experimental evaluation, making it a potent supplement to existing cloud storage schemes.

V. MODULE DESCRIPTION

Register:

This is our project's first module. For login purposes, the user updates their vital information in the database.

Login Information:

This is a module in our project that represents a unit of work conducted against a database within a database management system (or similar system) and treated in a coherent [9] and reliable manner independent of other transactions. A transaction is any update in the database where the user will transfer money to the supplier.

View of an Employee's File:

This module is intended to assist employees with viewing the branch manager's most recent file. The data base is represented by the file view.

Request From an Employee:

The employee will view the data file in this module. [10] And the Head-Office will be in charge of reviewing your case.

FILE DOWNLOAD FOR EMPLOYEES:

In this module, the employee will also be able to download a data file that contains [11] fully analysed data from a category-by-category perspective. Your file will be stored in a database, and an employee will be in charge of it.

File-Upload Manager:
This module is used to assist the user in uploading a file containing the land longitude, and the user will then update the report with their Thoughts, which will be saved in the database.

File View In Manager:
This module assists the [12] management in uploading files to the database. The manager must now view the file that he has uploaded. The file will then be viewed by him.

Head-Office Request-View:
The purpose of this module is to [12] assist the Head-Office in viewing user requests in the database.

Response from the Head Office:
The data file will be viewed by the Head-Office in this module. And, based on the results of the analysis, the Head-Office will be in charge of your file in the database. [13] The user's request is then responded to by the head office.

Hacker Opinion:
This module assists the management with uploading files to the database. The manager must now view the file that he has uploaded. The file will then be viewed by him.

Hacker Request:
The employee will view the data file in this module. And it [14] would be the responsibility of the Head-Office to review your file for Response [15].

VI. CONCLUSION

In this research, we provide the forward-pleasant puncturable evidence generally based on encryption plot, which is a cryptographic rough. Then, to fire up the construction, we provide a considerable enhancement of the updated AES design. Finally, we conduct the proposed MAES and give various preparation results in order to demonstrate its applicability. To grasp plausible advanced secrets of cloud email architectures in this paper.

References

[1] The Radicati Group Inc., "Cloud Email and Collaboration-Market Quadrant 2019," https://www.radicati.com/wp/wp-content/uploads/2019/03/ Cloud-Email-and-Collaboration-Market-Quadrant-2019-Brochure. pdf, March 2019, accessed April 8, 2019.

[2] Tim Sadler, "The Year of Email Data Breaches," https://www.infosecurity magazine.com/opinions/2017-email-data-breaches/, January 2018, accessed September 11,2019

[3] Wikileaks, "Hillary Clinton Email Archive," https://wikileaks.org/clintonemails/, accessed April 8, 2019.

[4] "The Podesta Emails," https://wikileaks.org/ podesta-emails/, April 8, 2020.

[5] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format," https://tools.ietf.org/html/ rfc4880, November 2007, RFC 4880 (Proposed Standard).

[6] B. Ramsdell and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," https: //tools.ietf.org/html/rfc5751, January 2020, RFC 5751 (Proposed Standard).

[7] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in 2017 IEEE Symposium on Security and Privacy. IEEE, 2017, pp. 137– 153.

[8] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons. (2021) Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. Available: https://arxiv.org/pdf/ 1510.08555.pdf

[9] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why johnny still can't encrypt: evaluating the usability of email encryption software," in Symposium On Usable Privacy and Security, 2021.

[10] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology–CRYPTO 2020. Springer, 2020, pp. 47– 53.

[11] Proofpoint, "Proofpoint Email Protection," https://www. proofpoint.com/us/products/email-protection,April 18, 2019.

[12] DataMotion, "DataMotion SecureMail," https://www.proofpoint. com/us/products/email-protection, April 18, 2019.

[13] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: secure messaging," in 2018 IEEE Symposium on Security and Privacy. IEEE, 2018, pp. 232–249.

[14] H.-M. Sun,B.-T. Hsieh, and H.-J. Hwang, "Secure e-mail protocols providing perfect forward secrecy," IEEE Communications Letters, vol. 9, no. 1, pp. 58–60, 2017.

[15] J. O. Kwon, I. R. Jeong, and D. H. Lee, "A forward-secure e-mail protocol without certificated public keys," Information Sciences, vol. 179, no. 24, pp. 4227–4231, 2019.