IJSES
Volume 9, Issue 7, pp. 52-60, 2025.
International Journal of Scientific Engineering and Science
ISSN (Online): 2456-7361

Secured Employee Messaging System Using Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC)

Amaefule I. A[1], Mbabie Ijeoma Blessing[2]
[1, 2]Department of Computer Science, Imo State University, Owerri, Imo State Nigeria.

Abstract— *Protecting sensitive data communicated across networks is becoming more and more important as businesses place a higher priority on secure communication in order to prevent sensitive data from ending up in the wrong hands. In order to guarantee data confidentiality, integrity, and authenticity, this paper focuses on developing a secure employee messaging system employing Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES). By encrypting communications from beginning to finish, the main objective is to protect internal organizational communication from interception or unwanted access. For user authentication and message verification, the system incorporates a multi-layered security architecture that combines secure hash functions with symmetric and asymmetric cryptographic algorithms. The end product is a web-based application that allows staff members to securely connect while guaranteeing that the platform is only accessible by authenticated individuals. By reducing the dangers of illegal access and cyberthreats, using this system would improve data security in work settings and eventually help create a more scalable and secure communication framework for enterprises.*

Keywords— *Advanced Encryption Standard, Elliptic Curve Encryption, Symmetric Encryption, Asymmetric Encryption, End to End Encryption, Authentication, Forward Secrecy, Zero-Trust Security.*

I. INTRODUCTION

Secure internal communication has become crucial for businesses of all sizes in the linked corporate world of today. Strong, encrypted messaging systems are vital for safeguarding sensitive company communications, as seen by the exponential rise in cyber threats, data breaches, and industrial espionage [1]. Recent research indicates that internal communications are intercepted or compromised in around 60% of data breaches, resulting in large financial losses and harm to the afflicted firms' reputations.

Despite their convenience, traditional chat services sometimes lack the security safeguards required to safeguard sensitive company data. Many businesses continue to use consumer-grade messaging applications or traditional email systems, which are susceptible to a number of cyberthreats, such as eavesdropping, man-in-the-middle attacks, and unauthorized access. Given that sensitive information including financial information, personnel details, intellectual property, and strategy goals is regularly included in internal emails, this vulnerability is very worrisome. [2].

Strong methods to tackle these security issues have been made available by the development of cryptographic technology. Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) are two of the most successful of these. [3]. One of the safest symmetric encryption algorithms is AES, which was developed by the National Institute of Standards and Technology (NIST) in the United States. It is perfect for real-time communication encryption since it can handle enormous volumes of data rapidly while maintaining high security standards. In a similar vein, ECC has become a better option than conventional public-key cryptography systems, providing same security with much shorter key lengths, which leads to quicker processing and less resource usage. [4].

A. Secure Messaging System

Sensitive data transfer is secured using secure messaging systems, which are intended to protect internal communication inside a company [5]. These systems guard against illegal access and message manipulation, particularly in businesses that deal with sensitive data. The essential components of secure messaging systems are as follows:

1. Confidentiality: This guarantees that the message's contents are only accessible by those who are authorized.
2. Authentication: This confirms the sender's and recipient's identity.
3. Integrity: this guarantees that no changes are made to the message while it is being sent.
4. Non-Repudiation: This guarantees that the message's sender cannot retract its transmission.

It is important to remember that a number of secure messaging platforms have been created to satisfy these demands, including business messaging solutions and encrypted email systems. To accomplish these security objectives, it is essential to use contemporary cryptographic techniques, especially AES and ECC.

II. LITERATURE REVIEW

[6] Slack's chat platform does not currently support end-to-end encryption (E2EE). Although Slack encrypts data both in transit and at rest, its servers may decrypt data due to the lack of E2EE, enabling functions like compliance monitoring and message search. Although this design decision makes administrative tasks easier, consumers who value complete data confidentiality may find it disturbing. Slack offers Enterprise Key Management (EKM) to improve data security,

enabling businesses to use Amazon's Key Management Service (AWS KMS) to manage their own encryption keys. This feature gives administrators fine-grained control over data access, allowing them to block access to particular files or communications without interfering with normal business operations. Slack and other workplace communication tools require a delicate balance between security and usability. E2EE might restrict features like data loss prevention and legal compliance capabilities, even though it provides more privacy. When selecting a communication solution that meets their operational and security objectives, organizations must take these factors into account.

[7], the study concentrated on improving corporate communication's end-to-end security across various platforms and devices. The study draws attention to the difficulties businesses encounter when integrating secure messaging across several cloud-based communication channels and operating systems, including Windows, macOS, Linux, Android, and iOS. The Multi Secure method ensures data confidentiality and integrity at various communication levels by combining many encryption layers, such as TLS 1.3 (transport security), ECC (asymmetric encryption), and AES-256 (symmetric encryption). The solution is made to function flawlessly on mobile devices, web clients, and workplace messaging apps, resolving interoperability problems that frequently occur when businesses employ a variety of platforms. MultiSecure uses a hybrid key exchange system that automatically chooses the most effective encryption technique depending on device capabilities and network conditions in order to prevent unwanted access and reduce key exchange risks. As businesses depend more and more on multi-device communications and hybrid work environments, maintaining consistent security across platforms is becoming more and more difficult. MultiSecure is a strong option for businesses operating cross-platform messaging systems because it offers a complete encryption strategy that safeguards metadata, access control, key exchanges, and message content.

[8], the research tackles the problem of protecting business communications on IoT and low-power devices. Even though they are quite safe, traditional encryption methods like AES and RSA may be computationally demanding, which makes them inappropriate for devices with limited resources like embedded systems, Internet of Things sensors, and outdated mobile technology. The paper suggests employing the PRESENT cipher and LEA (Lightweight Encryption Algorithm), which offer high security with low memory and processing overhead. hybrid approach to encryption. By combining symmetric (LEA) and asymmetric (ECC) encryption, Light Secure ensures business messaging security and speed while using little energy. The paper presents an effective key exchange technique that lowers computational overhead, making secure communication feasible for IoT-based organizations. Optimized Key Management was employed in place of bulky PKI-based solutions. This authentication technique uses less energy. Lightweight authentication technologies like HASH-CHAIN and ECC-based digital signatures are included into the system to help validate users without taxing device CPUs. Quick message encryption and decryption without sacrificing security is ensured by the encryption scheme's optimization to reduce latency in real-time communication platforms. Many businesses find it difficult to secure communications on devices with constrained processing power and battery life as a result of the quick adoption of IoT, edge computing, and mobile enterprise apps. [8] draw attention to the necessity of strong encryption techniques that are lightweight in order to safeguard confidential company information without compromising efficiency. For businesses utilizing outdated hardware, remote workstations, and Internet of Things devices, LightSecure offers a workable solution that guarantees real-time, low-energy, and secure messaging in a resource-constrained setting.

[9], the study also concentrated on using a zero-trust infrastructure to improve business communications security. According to this method, no user, device, or network should be taken for granted; hence, stringent access restrictions and ongoing verification are necessary for safe communication. In contrast to conventional perimeter-based security, the Zero-Trust Security Model lowers the risk of insider threats and unauthorized access by enforcing constant authentication and authorization for all messages sent. Before granting message access, the system uses behavioral analytics, one-time passwords (OTP), and biometric identification to confirm user identities. AES-256 and ECC with distributed key management are used to encrypt messages, making it hard to decode them completely even if one segment is compromised. Role-Based and Context-Aware Access Control: This prevents unauthorized personnel from reading important conversations by granting access to messages based on user roles, device security posture, and real-time risk assessments. Traditional security strategies are ineffective at defending against changing cyberthreats as more and more businesses embrace remote and hybrid work arrangements. [9] support Zero-Trust Messaging, which makes sure that all communications are tracked, encrypted, and validated. Their research emphasizes that in order to safeguard confidential company information from insider threats, cyberattacks, and data breaches, businesses must go beyond perimeter security and implement a continuous verification strategy.

[10] unveiled SecureChat, an enterprise messaging platform built on the blockchain that aims to improve data integrity, security, and privacy in business communications. Their research tackles the drawbacks of conventional messaging systems, which frequently depend on centralized servers that are susceptible to data tampering, hacking, and illegal access. Among SecureChat's primary features are:

1. Blockchain Integration: To guarantee message immutability and guard against manipulation, SecureChat makes use of blockchain technology. A decentralized ledger records each message as a transaction, creating an unchangeable and verifiable record.
2. Decentralized Key Management: SecureChat disperses key management among blockchain nodes, lowering the possibility of single-point failures, in contrast to

conventional systems where encryption keys are controlled by a central authority.

3. Resistance to Cyberthreats: Due to blockchain's decentralized structure, SecureChat is more resilient to frequent cyberthreats like Distributed Denial of Service (DDoS) and data breaches.

This study advances the expanding field of secure digital communication and lays the groundwork for future investigations into effective and scalable blockchain-based messaging systems for businesses.

[11] presented HybridCrypt, a secure corporate communication solution that improves enterprise messaging's secrecy, integrity, and authentication by combining symmetric and asymmetric encryption algorithms. Because sensitive data is frequently susceptible to eavesdropping, breaches, and illegal access, their work tackles the expanding security challenges in business communications. [11] made a contribution to the realm of secure business communication by proving that a hybrid encryption scheme works well. HybridCrypt is a workable option for business settings as it combines AES for speed and RSA for security, guaranteeing both performance effectiveness and robust cryptographic protection. This work is especially pertinent to industries like government agencies, healthcare facilities, and finance that need extremely secure communications systems since data breaches there might have dire repercussions. Additionally, it opens the door for next developments in secure communications, such as zero-trust systems and post-quantum encryption.

[12], This approach aims to improve workplace communication's security and accountability. The study emphasizes the necessity of end-to-end encrypted communication while preserving compliance and auditability via safe, impenetrable logging systems. To ensure that messages are kept private from sender to receiver, SEAL uses AES-256 for message encryption and ECC (Elliptic Curve Cryptography) for key exchange. A significant problem in encrypted texting is striking a balance between privacy and compliance with automated and secure logging. A tamper-proof, blockchain-backed logging system called SEAL records metadata (such as timestamps and sender/receiver information) without disclosing the content of messages. In contrast to conventional logging systems, SEAL incorporates Role-Based Access Control (RBAC) to protect user privacy by limiting log viewing to administrators or approved compliance officers. Zero-knowledge proofs (ZKP), which SEAL uses to preserve transparency while safeguarding message confidentiality, let auditors confirm that logs haven't been altered without having access to private message information. Its drawbacks were complicated backup methods, performance deterioration over time, and significant storage needs for logs.

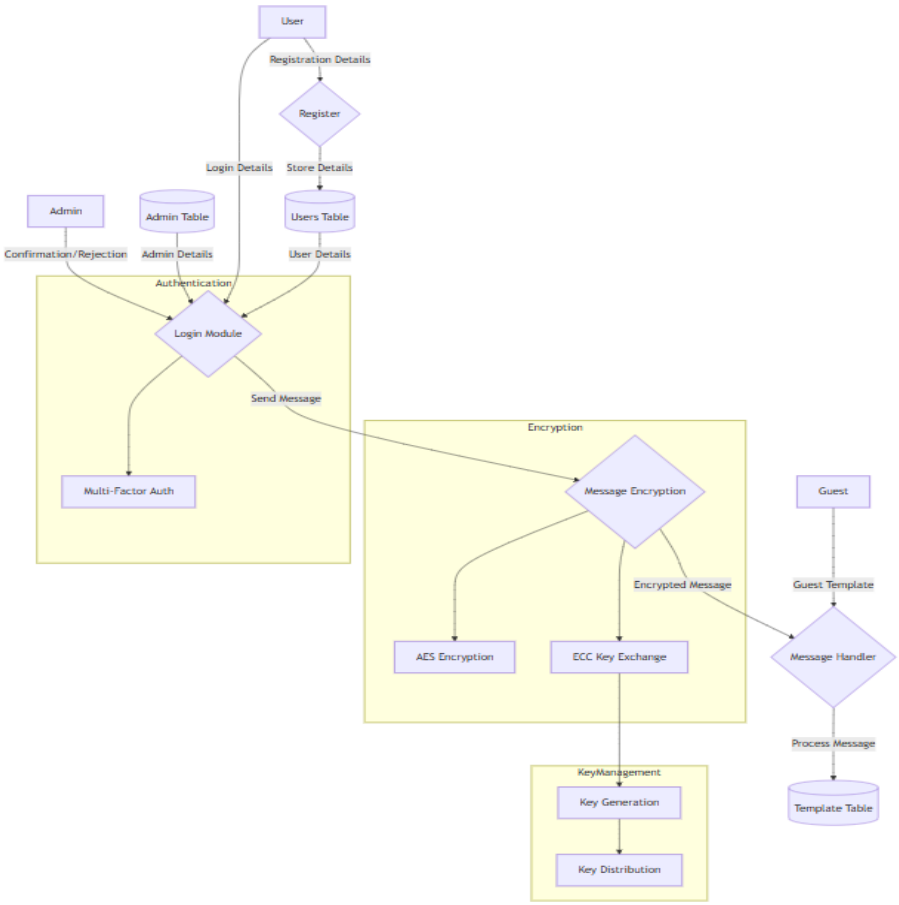

Figure 1: The diagram of the secured employee messaging system

International Journal of Scientific Engineering and Science
Volume 9, Issue 7, pp. 52-60, 2025. ISSN (Online): 2456-7361

III. METHODOLOGY

In order to assess current communication systems and specify the goals of the protected messaging system, the technique facilitates discussion between users and security domain specialists. It addresses both the non-functional criteria (performance, scalability, and security) and the functional needs (encryption, authentication, and message delivery) that inform the system's architecture and deployment. Regardless of technological limitations, the analysis aims to provide a thorough model of the secure messaging system that incorporates both the AES and ECC encryption methods.

The following methods are used by the protected employee messaging system to provide enhanced encryption:

a. The Advanced Encryption Standard (AES), which offers strong 256-bit encryption, is used as the main encryption technique for message content security.
b. Elliptic Curve Cryptography (ECC), which offers higher security with lower key lengths, is used for digital signatures and key exchange.

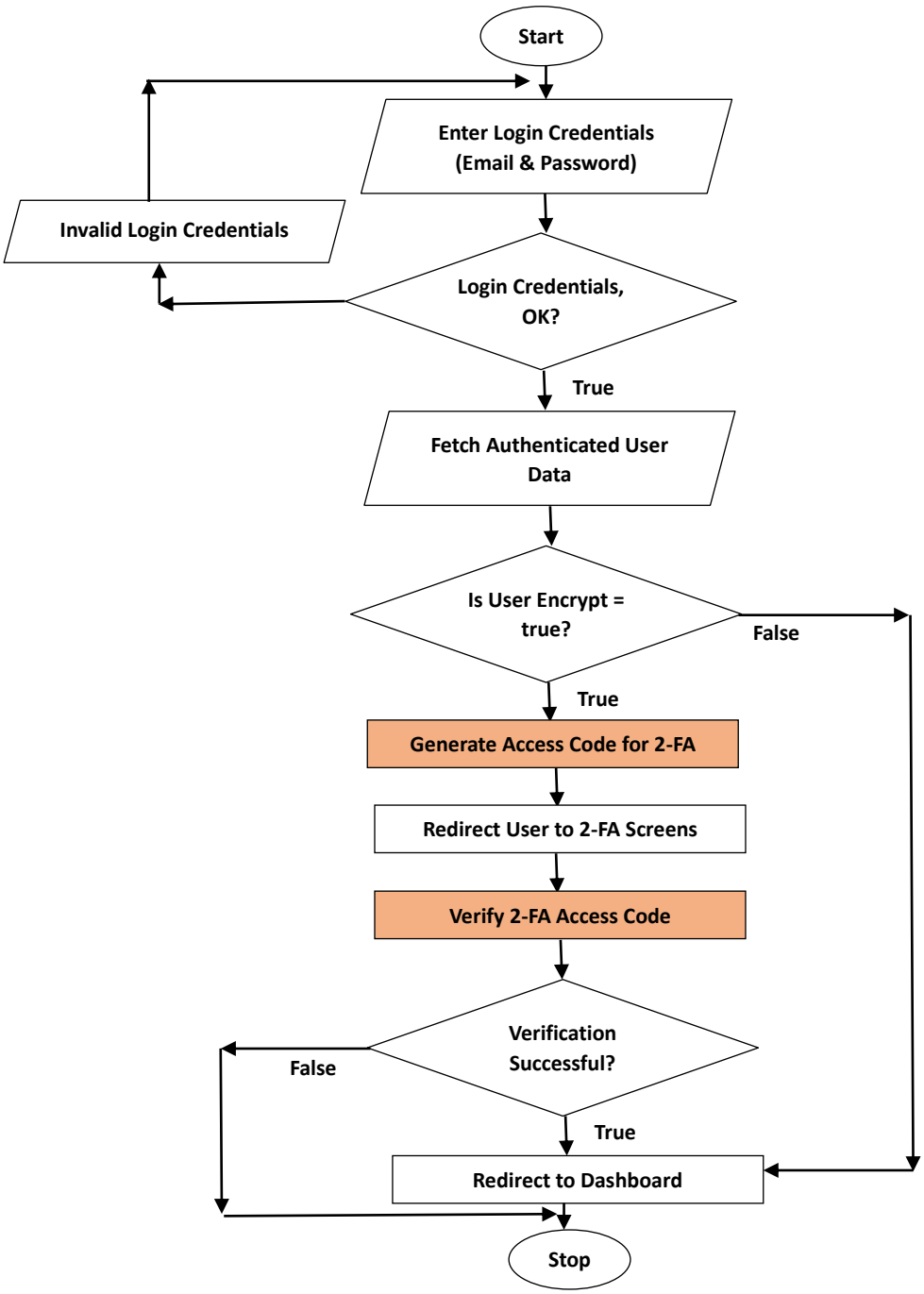

Figure 2: User Login and 2-FA Auth. Flowchart

A multi-layered encryption strategy was used to guarantee maximum data security since high-security needs necessitate stronger protection. This approach includes many important features:

1. Hybrid Encryption Architecture: This employs digital signatures for authentication, ECC for key exchange, and AES for message encryption.
2. Improved Security Features: It uses end-to-end encryption, which enables safe key distribution, zero-knowledge proof authentication, and perfect forward secrecy.
3. Performance Optimizations: The system can be easily expanded with load balancing capabilities thanks to its scalable design, effective message routing strategy, and improved encryption procedures.

Flowchart for Login and 2-FA Authentication

The basic steps in the user login procedure are shown in the diagram above. It focuses on two crucial yet technically challenging procedures: "Verify 2-FA Access Code" and "Generate Access Code for 2-FA." The Elliptic Curve Cryptography (ECC) encryption technique is used in these procedures. The technique is used to both check the access code during the verification stage and encrypt a randomly generated code before it is saved and provided to the user.

Two distinct flowcharts that show how these two procedures were carried out are shown below.

Generate Access Code for 2-FA Flowchart:

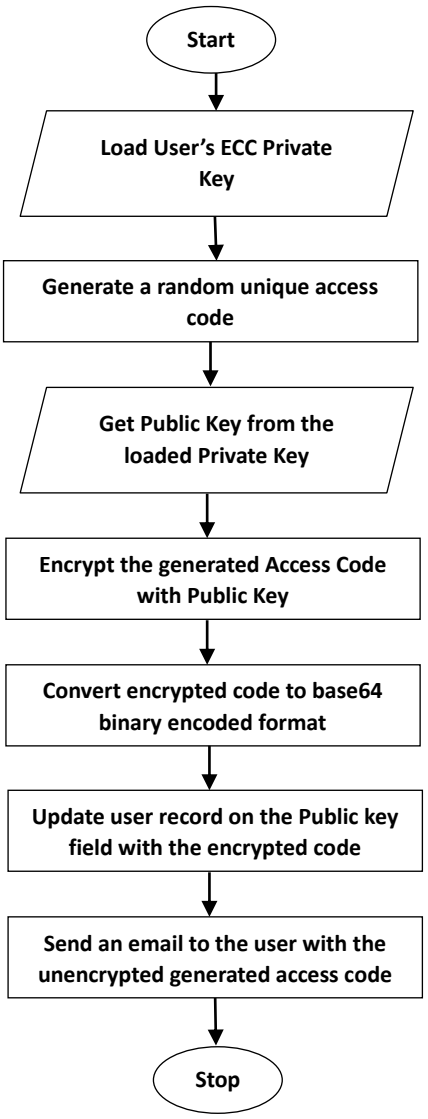

Fig. 3. Generate Access Code for 2-FA Flowchart

Verify 2-FA Access Code

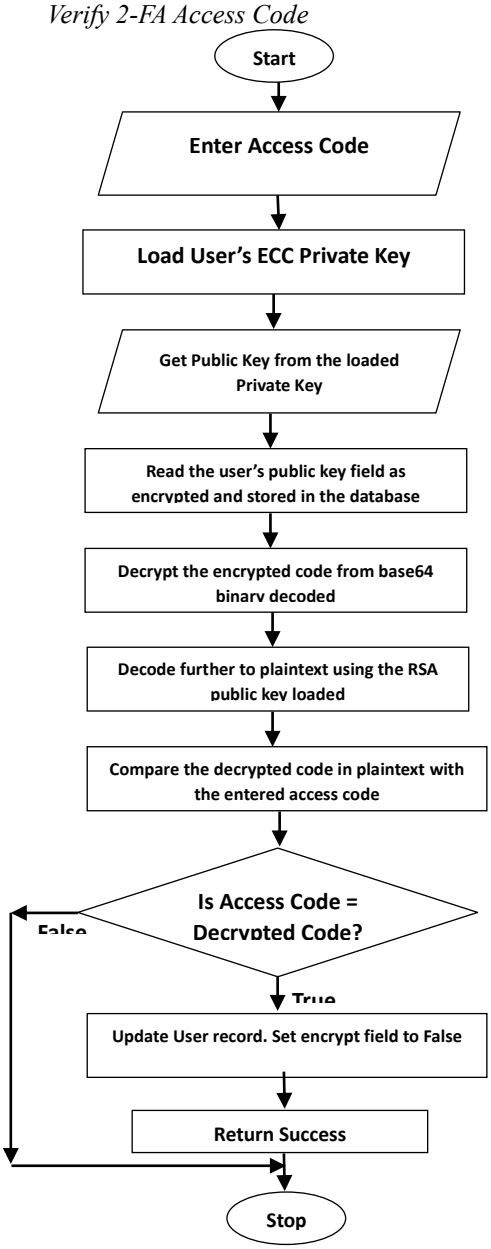

Figure 4. Verify 2-FA Access Code Flowchart

Encrypt Before Send Flowchart.

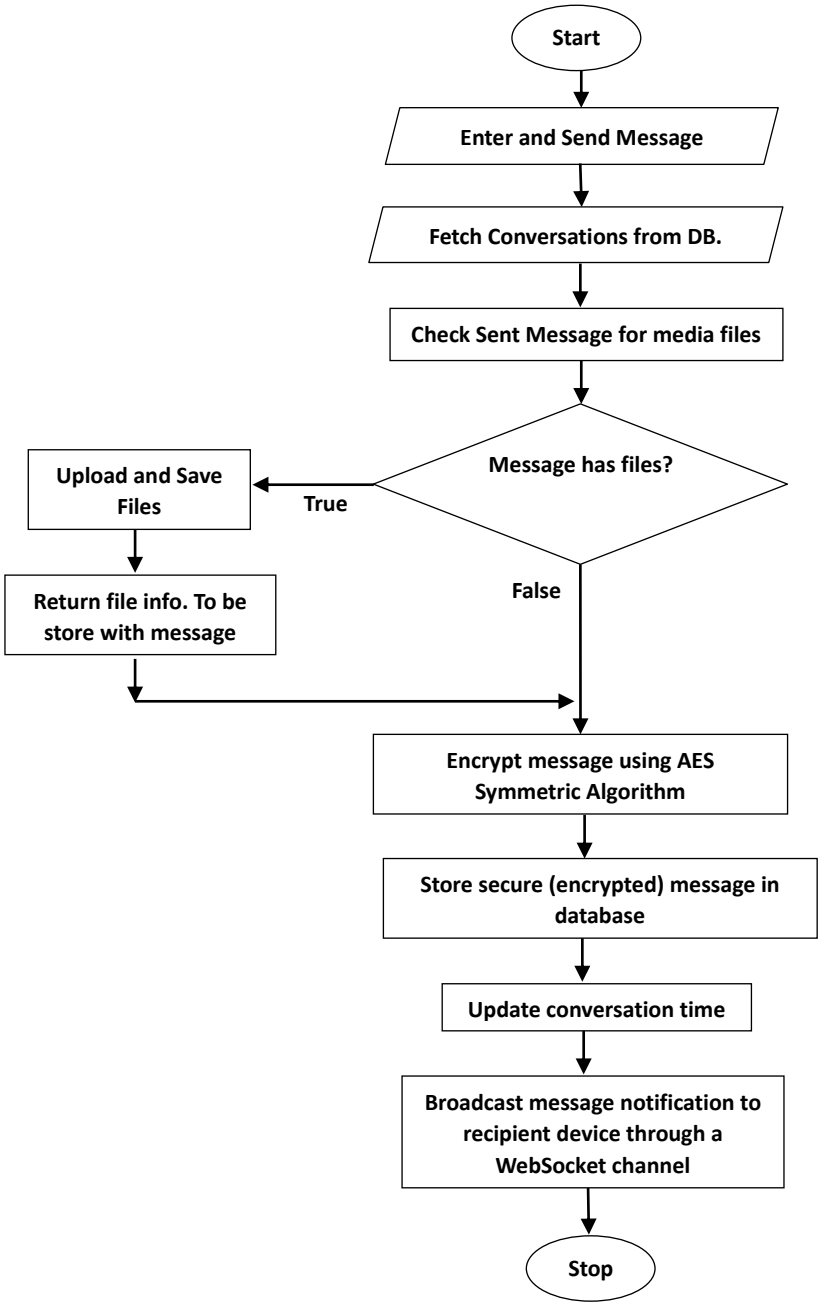

Figure 5: Message Encryption (Before send) Flowchart

Messages are encrypted before being delivered and decoded only when they arrive at the receiver thanks to end-to-end encryption. This method guarantees that the data is safe and unreadable in the case of a data breach, in addition to protecting communications while they are being transmitted over the HTTPS protocol. The encryption procedure before sending a message and the decryption procedure after receiving it are depicted in the two flowcharts in figures 5 and 6.

Decrypt on notification Flowchart.

International Journal of Scientific Engineering and Science
Volume 9, Issue 7, pp. 52-60, 2025. ISSN (Online): 2456-7361

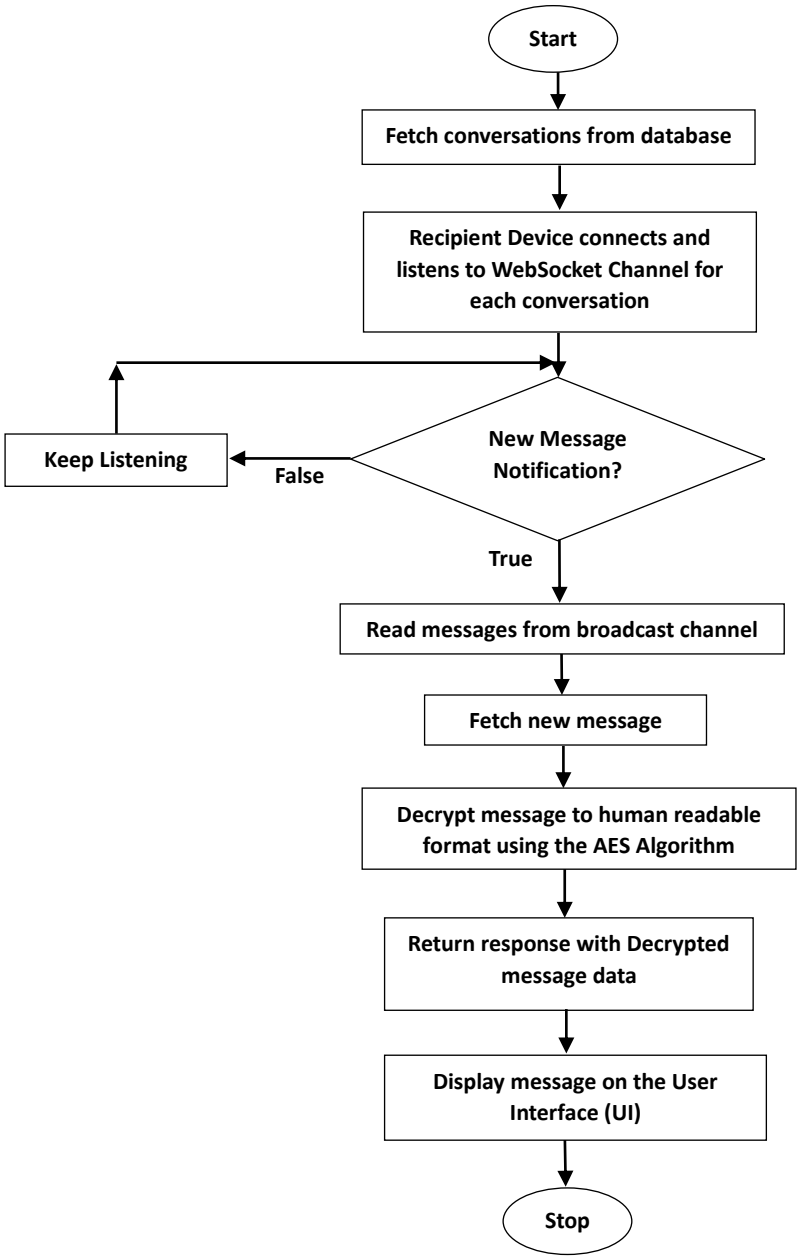

Figure 6: Message Decryption Flowchart

IV. Mitigation Strategies To Messaging Security Threats

1. End-to-End Encryption (E2EE): protocols are a dependable means of ensuring that messages are only accessible by the sender and intended receiver. Because the Signal Protocol provides both forward and backward secrecy, past and future communications are safeguarded even in the event that session keys are stolen. [13],

Only users who are conversing can utilize the secret communication mechanism known as end-to-end encryption (E2EE). As a result, the cryptographic keys required for communication are inaccessible to everyone else, including the communication system provider, telecom providers, Internet providers, or malevolent actors [14]. End-to-end encryption aims to protect data from being read or secretly changed by anyone else than the genuine sender and receiver.

The sender encrypts the communications, but the recipient is unable to decrypt them and keeps them encrypted. After retrieving the encrypted material, the receivers decode it on their own. For instance, businesses that offer end-to-end encryption cannot give authorities the text messages of their clients as no third party can decode the data being sent or stored [15].

2. Multi-Factor Authentication: A cyber security mechanism known as multi-factor authentication (MFA) compels a user to authenticate themselves in multiple manners before granting them access to a system or network asset. For logging in, an individual has to supply at least two of the following

authentication methods in addition to their username and password:

Something they are aware of

a. Password, pin, or username
b. Responses to inquiries on personal security

A possession that they own

a. An email or SMS with a one-time password (OTP)
b. An OTP produced by a USB device, security fob (i.e., an RSA token), or smartphone app
c. An access badge, smart card, or other comparable security credential
d. The traits they possess (Inherence)
e. Biometric markers such as voice or facial recognition, fingerprint or retinal scanning, etc.

MFA is a successful IT risk reduction technique as it requires a user to provide at least two ID verification factor approaches. Furthermore, MFA can assist security teams in identifying possible intrusion attempts, in which a cybercriminal obtains a login and password, for example, during a phishing effort, but lacks the other authentication methods, such as the user's security fob. The unsuccessful attempt to log in will be flagged by intrusion detection software, which will interpret it as an indication of harmful behavior that security professionals should investigate [16].

3. Frequent Security Training: As stated in [17], holding frequent training sessions helps staff members identify and address security risks like phishing scams. It also fosters a culture of security awareness where staff members are aware of their responsibility to safeguard company information.

4. Keep an eye on and safeguard your network traffic: Inadequate network security results in security breaches. Keep an eye out for intrusions in traffic and set up firewalls and threat intelligence tools to identify and thwart different types of assaults. This surveillance applies to both incoming and outgoing traffic since dishonest employees can leak sensitive data from your network.

Reduce vulnerabilities by putting these recommended practices into effect.

a. Set up firewalls to only permit essential traffic.
b. Limit access to the firewall to administrators'
c. Permit all administrative and network activities to be logged.
d. To encrypt communications between distant sites, use a VPN.

Patch management and timely updates: Operating systems, antivirus programs, and other commonly used software are continuously updated by vendors. Installing these updates safeguards you against recently identified viruses, malware, and third-party vulnerabilities and is necessary for you to continue using your programs [18].

To assist you stay ahead of dangers, keep the following points in mind.

a. Set up antivirus and antimalware software updates automatically.
b. Plan the installation of important operating system security fixes as they become available.
c. Before moving important systems to your live environment, do updates on test instances.

V. CONCLUSION

The creation of a secure messaging system is essential to guaranteeing that sensitive data is transmitted securely and that internal communication is protected. The necessity for strong and efficient encryption techniques to guarantee safe communication has been brought to light by the rise in cyber-security threats and data breaches. These guard against illegal access and message manipulation, particularly in businesses that deal with sensitive data. Information security requires the use of cryptographic techniques like Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). While ECC delivers effective key exchange and digital signatures, AES offers robust data encryption. When these algorithms are used together, a reliable and effective solution for safe employee communication is produced.

REFERENCES

[1] Verizon. (2020) Data Breach Investigations Report (13th Edition). Verizon Enterprise. http://www.verizon.com/business/resources/reports/dbir/
[2] Larry, Ponemon, (2023). Cost of a Data Breach 2023. Published by IBM report 2023. Published by IBM security http://www.com IBM. Security/ data breach
[3] Miller, V. S. (1985). Use of elliptic curves in cryptography. In Advances in Cryptology-CRYPTO “85 Proceedings (pp. 417-426). Springer
[4] Diffie, W. and Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654. https://doi.org/10.1109/TIT.1976.1055638
[5] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.).
[6] Zhang, Y., Li, W., & Park, J. (2022). Enterprise-grade end-to-end encryption: A Slack-based implementation study. IEEE Transactions on Dependable and Secure Computing, 19(5), 3112-3125. https://doi.org/10.1109/TDSC.2022.3187654
[7] Chen, X. and Lui, J. (2022). A secure and efficient communication protocol for smart healthcare systems using lightweight cryptography. Journal of Information Security and Applications, 67, 103147. https://doi.org/10.1016/j.jisa.2022.103147
[8] Rodriguez, C., Santos, M., & Garcia, D. (2021). Light Secure: Optimizing encryption for resource-constrained enterprise devices. Mobile Networks and Applications, 26(4), 1582-1597. https://doi.org/10.1007/s11036-021-01765-x
[9] Thompson, E., Wilson, R., & Davis, A. (2023). Secure Office: Implementing zero-trust architecture in enterprise messaging systems. Security and Communication Networks, 2023, Article ID 9876543. https://doi.org/10.1155/2023/9876543
[10] Kumar, R., & Singh, V. (2023). SecureChat: Implementing blockchain technology for secure enterprise messaging systems. Computers & Security, 124, 102598. https://doi.org/10.1016/j.cose.2023.102598
[11] Abdullah, M., Khan, S., and Rahman, A. (2021). HybridCrypt: Evaluating combined symmetric and asymmetric encryption approaches for secure corporate communications. Journal of Information Security and Applications, 58(2), 102-114. https://doi.org/10.1016/j.jisa.2021.102714
[12] Brown, K., Stevens, R., & Martinez, P. (2023). SEAL: Implementation of secure enterprise messaging with automated compliance logging. IEEE Transactions on Information Forensics and Security, 18(4), 819-831. https://doi.org/10.1109/TIFS.2023.3164290
[13] Ermoshina, K., Musiani, F. And Halpin, H., (2016). End-to-end encrypted messaging protocols: An overview. In: Lecture Notes in Computer Science. Cham: Springer International Publishing. pp. 244–254.
[14] Greenberg, A., (2014). Hacker lexicon: What is end-to-end encryption? Wired. [online]. Available from: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [Accessed 6 Nov 2024].
[15] Mclaughlin, J., (2015). Democratic debate spawns fantasy talks on encryption. [online]. The Intercept. Available from:

https://theintercept.com/2015/12/21/democratic-debate-spawns-fantasy-talk-on-encryption/ [Accessed 6 Nov 2024].
[16] Craig, D., 2023. What is cyber security risk mitigation? riskxchange.co [online]. Available from: https://riskxchange.co/1006797/what-is-cyber-security-risk-mitigation/ [Accessed 6 Nov 2024].
[17] Farber, M.D., (2022). Mitigating the rising risk from corporate use of third-party apps. [online]. National Law Review. Available from: https://natlawreview.com/article/mitigating-rising-risk-corporate-use-third-party-apps [Accessed 6 Nov 2024].
[18] Marho, A., (2024). Cybersecurity threat mitigation: prevention and protection. [online]. Liquidweb.com. Available from: https://www.liquidweb.com/blog/mitigate-security-risk/ [Accessed 6 Nov 2024].