Tec Empresarial
P-ISSN: 1659-2395; E-ISSN: 1659-3359

ACCESS CONTROL MECHANISM BASED MESSENGER APPLICATION FOR SECURE COMMUNICATION USING AES ENCRYPTION METHODOLOGY

Mrs.Mary Rexcy Asha
M.E., Associate Professor, Department of Information Technology, Panimalar Engineering College, Chennai, India.

Aishwariya S G
Department of Information Technology, Panimalar Engineering College, Chennai, India.

Charulatha B
Department of Information Technology, Panimalar Engineering College, Chennai, India

Nithyasri B
Department of Information Technology, Panimalar Engineering College, Chennai, India

ABSTRACT
Messaging application is among the most popular applications for smartphones. These essentially eliminate client's conversation expenses because they can initiate phone conversations and send texts via the Internet. Practically everyone who owns a smartphone uses these apps. Unfortunately, like every other type of application, the majority of these contain integrity and confidentiality flaws and can be attacked by hackers. Thus, the technology of using cryptography for transmitting information—in which the texts are encrypted and sent by the sender—makes this application unique. The encrypted message is also sent to the recipient. After the authentication and validation phase is finished, the message is decrypted. We employ the access control mechanism for this procedure. It is a system that restricts access to the decrypted message or message session to only those who are permitted. For the highest level of protection, we can employ the iris/face recognition technique. Only when the authenticated the individual's face matches the pre-registered credentials the message will be encrypted. The combination of encryption and access control mechanism offers this messaging app the highest level of privacy.

Keywords: Access Control Mechanism, Encryption, Cryptography, Authorization, Text

INTRODUCTION

The significance of security and privacy continues to increase in today's world of digital communication. People are depending on these platforms in order to conduct business, share personal information, and interact with friends and family as a result of the expansion of instantaneous messaging applications. But as a growing amount private information circulates on these online platforms, Users must be aware of the security precautions that have been put in to

safeguard their personal information. Encryption is one of the fundamental security features of message applications. The process of generating plaintext into ciphertext which can't be decrypted without the decryption key—is commonly referred to as encryption [1]. Smartphones have evolved into a vital fixture of the lives of individuals and priorities in the modern world. Messaging and conversation applications are the most popular applications. The majority of such apps fail to offer the required security and privacy for exchanging user data. Nevertheless, most mobile messaging applications offer End-to-End (E2E) safety [3] and privacy to their users. For Android-powered mobile devices, it is recommended to use an end-to-end encrypted secure messaging app. In the suggested application, the ECDH technique is employed to generate the key pair and exchange that yields the shared key needed for symmetric data encryption algorithms. When utilizing the recommended Application, users can share text messages, voice messages, and photos. Text message security is achieved using the standard AES technique with a 128-bit key [2].

LITERATURE SURVEY

S. Srinivasan, S. Sahoo, and S. S. Raj, "Secure Sharing of Multimedia Content using Attribute-Based Encryption in Mobile Messenger Applications", (2022). The paper suggests employing attribute-based encryption (ABE) to address the issue of safe audio and video sharing in mobile chat apps. ABE encryption is a kind that permits information to be encoded using the recipient's place of residence, race, or decades of age, among other variables. This enables the encryption of info for a particular recipient class based on criteria. The suggested solution is assessed by the authors against other comparable systems using a range of performance measures, including encryption and decryption times. [1]

The IEEE Transactions on Dependable and Secure Computing are proposing "Privacy-Preserving Access Control for Cloud-Based Instant Messaging Services," which was made by H. Shang, W. Li, Z. Liu, and H. Jin (2022).In order to preserve users' privacy, this article suggests a secure attribute-based access control (PPABAC) system and attribute-based encryption (ABE) for cloud-based instant messaging services. The suggested method enables individuals to set constraints on access according to their characteristics (e.g., gender, place of residence, employment), and the cloud-based service enforces the policies without disclosing the characteristics or access controls of the users. Because of the mechanism's provision for particular control of access, individuals can decide which people or groups to offer data with depending on certain qualities. Creators of cloud-based instant messaging services looking to offer precise access control while safeguarding customers' privacy may find the suggested method helpful.[2]

C. Kim, H. K. Lee, and H. G. Kim, "Secure and User-Friendly Access Control for End-to-End Encrypted Instant Messaging," International Journal of Security and Networks, 2021. This study suggests an entire encrypted instant messaging (IM) system's secure and intuitive access control mechanism. [3] Users can maintain acquaintances and set access control restrictions for their chats using the suggested system, which is based on the access control list (ACL) model. The access

control policies are implemented locally on the users' devices, and the ACLs are kept in a safe key-value database.

A. Ramamoorthy and P. Jayagowri, "A secure public key cryptosystem based medical records using non-commutative group," Journal of Physics: Conference Series, 2021.[4] This study served as a major contribution to modern digital signatures, brought about an upsurge in the field, and charted a new course for public key encryption. Ever since its inception over two decades ago, DES has emerged as the most widely utilized packet encryption method for data globally. Long resistant to cryptography, DES was finally cracked in 2007 as a result of advancements in offensive technology. Later, differential analysis was used to create triple DES and reformatted DES, which are resistant to attacks. Because triple DES uses three different keys to encrypt data blocks three times, it is more secure than triple standard encryption and has an efficiency comparable to 112-bit keys.[11]

The International Journal of Engineering and Advanced Technology proposed R. Gayathri and C. Kalieswari in 2020. [5] This study presents two different encryption of databases approaches.Both approaches make use of the RSA algorithm. The first type of encryption scheme is field-based. Every field are exposed via the user's master key. Next, it displays record-oriented encryption. A single master key is utilized. This method was applied to subsets and groups of integers. The security of the database is one of the more challenging problems. Often, asymmetric cryptosystems are utilized in this capacity. Data is effectively written into protected locations using encryption keys. This study claims that the chat app provides a more robust and flexible curriculum constructed with modern technology in order to provide a reliable system, for discussion. [10]

Rizki Fauzian, Devie Pratama Subiyanti, and Diotra Henriyan's "Designing and deploying a real-time web-based chat server" was released by the International Conference on Engineering and Technology in 2016. This research article suggests that a conversation program should be multi-site and feature a live forum to serve a sizable user base. The Node.js server and the MongoDB website were developed using this foundationally specified programming syntax. The main disadvantage of using node.js is that we have to incorporate other third-party libraries, such as "socket," with the goal to make the app real-time. Because Firebase contains all the components required to operate as a real-time usage, it does not require libraries. [6]

Shabnam Bano and Mohd Atiq published "Secure and Efficient Data Storage and Access in Cloud Using AES Encryption Algorithm" in the International Journal of Computer Applications in Technology in 2021. This work uses the AES encryption technique to provide a reliable and efficient method of data access and management in cloud-based settings. The authors show that by combining symmetric and asymmetric encryption algorithms with safe key management procedures, the suggested approach may attain substantial levels of safety while facilitating data access. The usefulness of the suggested technique in terms of efficiency and safety is demonstrated by the experimental findings offered in the paper. In summary, this work makes a significant

contribution to the subject of cloud security and offers insights into how to apply AES encryption in cloud settings for safe and effective retrieval and management.[9]

“AES Encryption Algorithm for Cloud Security” by Saurabh Yadav and Ankit Jain (2019). Additionally, Yadav and Jain compare AES with other encryption algorithms that are frequently used in cloud computing, like RSA, Blowfish, and DES.[8][4] They come to the conclusion that Encryption is a more effective and safe method for transmitting and storing information in the cloud. The authors then suggest an architecture for safe data storage in the cloud that encrypts data using AES. Data is encrypted by the framework prior to it gets transmitted to the cloud as well as is decrypted when it is retrieved. Additionally, the authors recommend using key management systems to guarantee safe key storage and distribution. Lastly, Yadav and Jain talk about the drawbacks of the AES encryption method, including the possibility of side channel and brute force attacks. They contend that more effective defence against risks to cloud security can be achieved by combining encryption with additional security measures including control of access, authentication, and auditing.

Rachmat, N. [14] demonstrates the fact that in order to design an extremely safe Android application, the programme developer should take into account a number of variables in along with security and performance. The Android platform's application performance is in need of improvement due to the constrained resources of Android handsets. If algorithms perform better on Android is a common question in many development communities such as Stack Overflow and Quora. This work aims to analyze the performance of the three most prominent safe encryption algorithms—Rijndael, Serpent, and Twofish—to address the issues stated in order to identify which of them is the best to be implemented in Android handsets. Devices that measure the computational cost and performance of the CPU are used to conduct the test. [20]

Sagheer and Ali, A. [15] An end-to-end encrypted secure messaging app for smartphones running Android is recommended in this study. This is achieved using public key cryptography techniques. The Elliptic Curve Diffie Hellman Key Exchange (ECDH) algorithm was used by the proposed application to generate the shared key that would be used for data encryption utilizing symmetric approaches. Using the recommended Application, users can converse via voice conversations, text messages, and photos. [19] For text message security, a 128 bits key and the widely used AES algorithm are used. The 160-bit length of the generated key was shortened to 128 bits by selecting the first 16 bytes of the key.

Due to the rapid advancement of the internet and the increasing popularity of e-commerce, Lu, Z [16] created data encryption technology, which is now playing a crucial role in data security. Information security consists of two parts: safety protocols and cryptographic algorithms, the latter of which is the underlying technology. The Advanced Encryption Standard (AES) encryption method is among the most popular symmetric encryption methods.

Muhammad Shiraz et al. [17] suggested that it is challenging to outsource private and sensitive data to distant data centers because of growing worries about data safety and confidentiality. A few key elements of the framework this study presents are enhanced safety and owner-data privacy. By modifying the 128 AES algorithm, the double round key feature speeds up encryption to 1000 blocks per second. However, the conventional method is to use a single round key that can process 800 blocks per second. The recommended method enhances network resource management, boosts trust, and uses less energy while offering better load balancing. The recommended framework specifies that AES be used with text widths of 16, 32, 64, and 128 bytes.[12]

These algorithms exhibit issues when applied to key administration and security functions. This paper emphasizes a methodical examination of these issues in addition to describing the implementation, full the application, and technique comparison with other current approaches of the AES algorithm. One of the primary drawbacks of using node is that we have to integrate extra third-party libraries like "socket" in order to make the application real-time. Firebase has everything required to operate like an application in real time integrated right into it, thus libraries are not needed.[18]

SYSTEM ARCHITECTURE

The operation is supported by several kinds of subsystems, which can be thought of as commands that, when correctly integrated, produce the intended outcome from the implementation point of view. Two such fundamental subsystems that stand out are the encryption and decryption subsystems. These subsystems are independent entities that receive the secret key, the ciphertext or the clear message as inputs, and provide an encrypted or decoded result as an output. The AES cryptographic algorithm's mathematical model is directly implemented throughout the calculation phase.

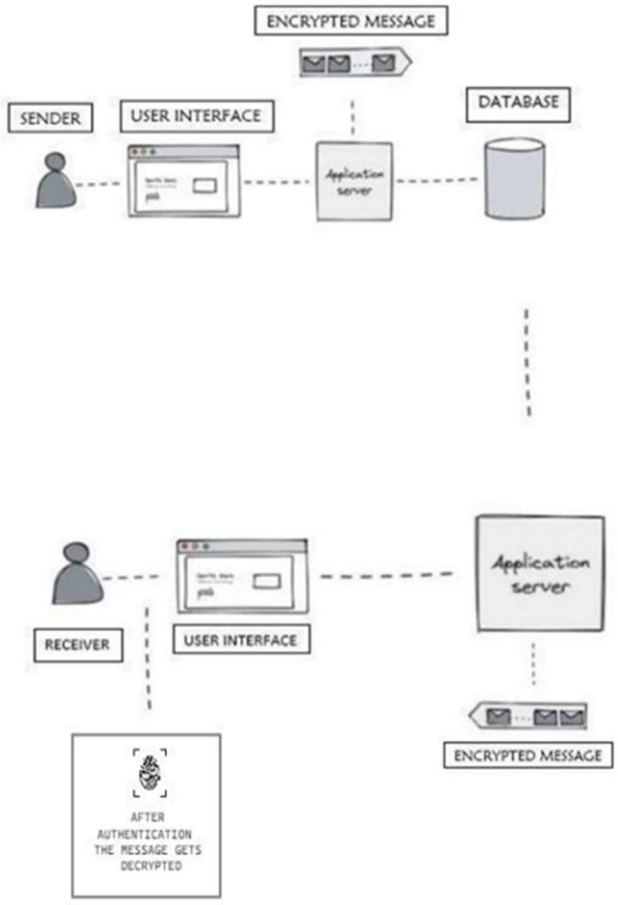

Figure 1. System Architecture

EXISTING SYSTEM

WhatsApp is a popular messaging application that enables users to send and receive voice and text messages, multimedia files, and internet-based voice and video calls to an individual or a group. With end-to-end encryption enabled by WhatsApp, messages are only readable by the person who sent them and their intended recipient. WhatsApp uses end-to-end encryption for all of its calls and messages, so only the person who sent them and the recipient can see the contents of the exchange. WhatsApp has faced privacy issues, notably after modifications in its privacy policy in 2021.

The policy changes caused some criticism and caused people to go to other chat programs. Numerous operating systems, including web browsers, iOS, Android, and Windows Phone, are compatible with WhatsApp. WhatsApp is one of the most widely used messaging programs worldwide, boasting billions of active users worldwide. With the "Status" function, users can communicate with their connections by sending texts, images, and videos that vanish after a day.

Despite being created with customer convenience in mind, WhatsApp poses serious privacy issues. Although end-to-end encryption guarantees the security of messages while they are in transit, it

gathers a variety of user data, including contact information, device data, and even location data. Given that WhatsApp and Facebook are associated, this collecting becomes even more concerning because user data is frequently shared between the two organizations.

This method raises questions about how personal data may be misused for unapproved surveillance, targeted advertising, or algorithmic manipulation. Even with its strong encryption defences, WhatsApp is not resistant to security flaws. Users' money and personal information is at risk due to the rise in reports of hacking events, phishing attempts, and malware distribution over the site. These vulnerabilities have been used by cybercriminals to distribute harmful software, obtain unauthorized access to accounts, and even plan identity theft. Thus we consider that these are the main backlogs for the existing messaging applications.

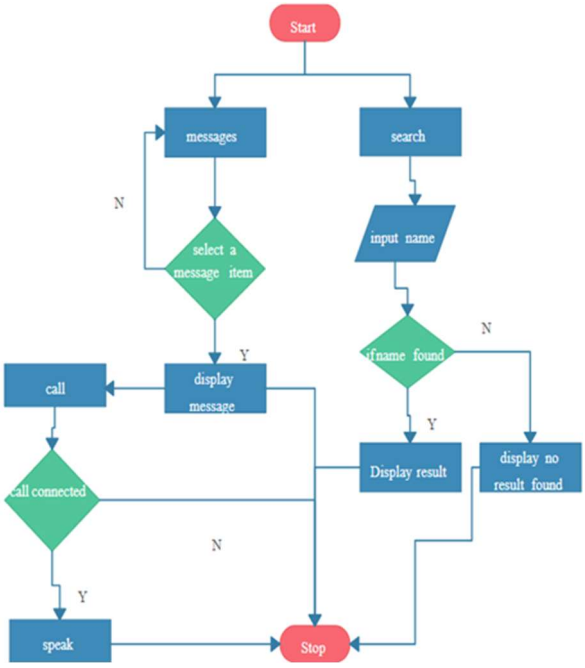

Figure 2. Flowchart of Existing System

PROPOSED SYSTEM

The individual can rapidly and simply log into the messaging application by entering a password with the help of Face ID to set up a connection. This could enhance the overall user experience and make using the app simpler and more convenient. Furthermore, since each user's face is distinct, Face ID adds an additional layer of authentication to the app's security that goes beyond passwords.

Turning on Face ID: The user's device must initially have Face ID activated on. Usually, you may accomplish this in the device's menus.

Commencing the session: The user must launch the messaging application and initiate the Face ID identification procedure in order to begin a session.

Face scanning: The gadget is going to examine the individual's face using its front-facing camera. In order to verify that the user is the one wishing to begin the session, this is done.

Authentication: the gadget will examine the user's identification and launch a fresh messaging connection for them if their facial check matches the saved face data. The user will be prompted to try again or use an alternative authentication method if the facial scan does not correspond to the stored data and the authentication fails.

Session established: The messaging application will begin another conversation when the user's identification has been verified, lasting 20 seconds. It then continues to check the user's identity every 20 seconds. After the user's identity has been verified, the communications can be decrypted and viewed by the user.

The application is visually appealing and simple to operate with an interactive user interface. The app must be downloaded by the individual using it from the platform on which it is being released. (As the Play Store does). After activating the application, the user should use their phone number to register. They will receive an OTP for confirmation. The user has to enter his Face ID or Touch ID after logging into his account and confirming that it has been successfully approved. By using Touch ID or Face ID, the user can easily and quickly login into the messaging application without having to enter a password. This can improve user happiness and make the program easier to use and more practical.

Furthermore, because each user's face is unique and provides additional authentication than a password, using Touch ID or Face ID for authentication enhances the protection of the program.

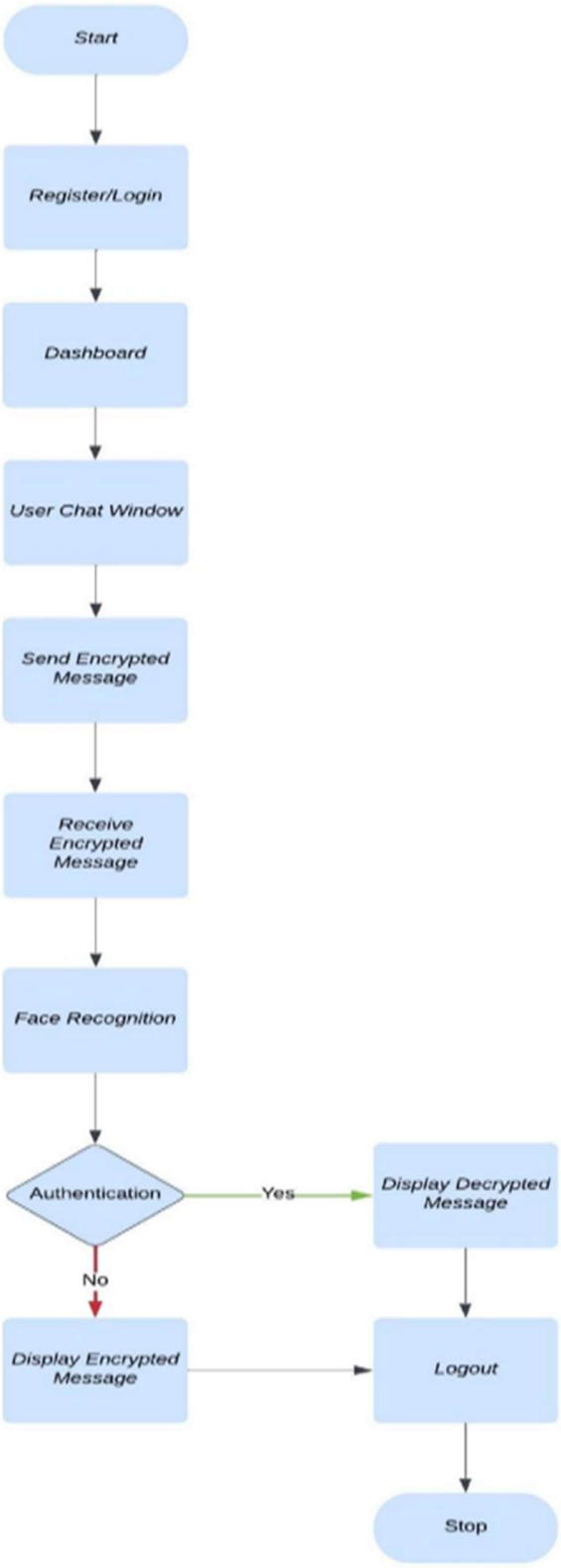

Figure 3. Flowchart of proposed System

ACCESS CONTROL

We've incorporated access control to the messaging application in addition to the encryption to make ensure only those with authorization may access it. [4]. Stronger authentication techniques like password-based, two-factor, or biometric authentication are included in this, depending on the specifications of the application. This keeps unwanted users from accessing the application and guarantees that only authorized users are able to join the conversation.

In order to guarantee that users only view messages that they are authorized to view, we have additionally added restriction of access at the user's message level. This implies that even in the unlikely event that an attacker manages to access the program, they will be unable to read messages that they are not supposed to.[12]

All things considered, we've put in place a strong security framework to guarantee the integrity and confidentiality of your communications.

ACCESS CONTROL BASED SECURE COMMUNICATION:

In a circumstance deemed secure and confidential, information can only be accessed and shared by authorized individuals using an approach known as access control based secure communication. It is a crucial part of the information protection, especially in enterprises that deal with confidential data. Restricting access to information to those who are authorized is the aim of access control based secure communication. This is accomplished by implementing several kinds of security measures, including encryption, authorization, and authentication. Verifying a user's or system's identity is called authentication.

Typically, in order to achieve this, someone must supply a user name, login credentials, or another form of identity, such as a biometric scan. The system might decide what level of access a user should be given after they have successfully authenticated.

Offering authenticated individual’s specific privileges is a form of authorization. Usually, to do this, individuals are given responsibilities and authorizations according to their level of authority or work function. For instance, a supervisor might only have exposure to essential info about customers, whereas a representative from customer service may have access to critical financial information.

The process of transforming plaintext information into ciphertext in order to prevent unwanted access is known as encryption. Usually, a cryptographic procedure is used for this, making sure that only people with the right key may decrypt the data. Secure interaction that is based on access control is crucial for preventing unwanted access to private data. Additionally, it can assist firms in adhering to laws like PCI DSS, GDPR, and HIPAA, which mandate that specific kinds of data be secured and accessible only to those who are permitted. Secure communication based on access control can be implemented in a number of ways. Using a Virtual Private Network (VPN), which offers a safe passage between multiple endpoints and enables data to be transferred over the

internet securely, is one popular technique. Utilizing Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption, which encodes data in transit to shield it from manipulation and interception, is an additional technique.

METHODOLOGY

In today's digital age, secure messaging has become essential to ensure reliable interaction with others. To avoid an intruder or sniffer from accessing an original interaction, it must be encrypted to make it incomprehensible to everybody. It prohibits intruders from capturing or altering the content of the message. The message can only be read by the person who holds the unique passcode.

Thus, protected Messaging requires the use of cryptographic methods. This approach provides both safety and accessibility as well. The transmission of messages over networks is vulnerable to threats such as illegal entry and surveillance. The content of the message could be captured or modified by an intruder during transmission. Using cryptographic techniques prior to transmission can help reduce the risk. The encryption algorithm that had been employed is the Advance Encryption Standard (AES) algorithm.

AES ALGORITHM

The Advanced Encryption Standard (AES) is an extensively utilized method of encryption which offers an exceptionally high level of security for electronic data. The specific key is employed for encryption and decryption in the symmetric key mechanism used by AES encryption. This key is generated on each gadget of the users who take part and is not retained by the messenger application's server. during the conversation. It is essential for privacy on computers, data protection, and government cybersecurity. In an attempt to provide their users with an unprecedented level of protection as well as safeguard their communications from modification and possible monitoring, these programs employ AES encryption. It's important to keep in consideration that as though AES encryption provides a high level of security, it is not unbreakable.

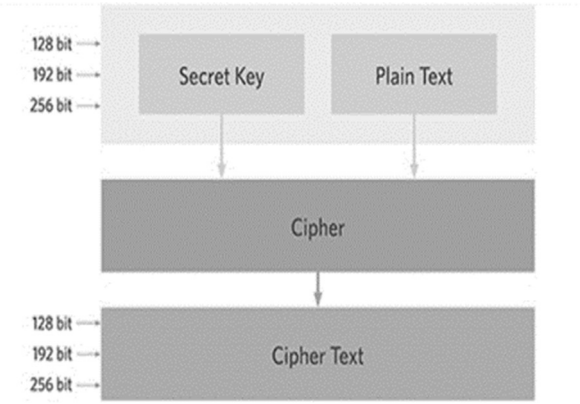

Figure 4. AES Design

FRAMEWORK MODEL

An encryption algorithm designated as the Advanced Encryption Standard (AES) concept uses symmetric keys via fixed block sizes of 16 bytes and key sizes of 128, 192, and 256 bits. The four primary operations of the AES algorithm are AddRoundKey, MixColumns, SubBytes, and ShiftRows. The total amount of loops in which these operations are performed depends on the size of the key. A plaintext message that is separated into 128-bit blocks is the input used by the AES algorithm. Every block is sequentially processed via the four processes, with a new key being utilized for every iteration.

The encrypted message, or ciphertext, is what's left over after the final round. Sensitive data is frequently secured using the AES paradigm, which offers a resilient level of defence against assaults. The recipient receives the plain text that was sent by the sender, which is subsequently ciphered and saved on the encryption server. To decrypt the cipher text, the recipient must receive the secret key from the sender over a secure channel. It transforms the encrypted cipher text into plain text.

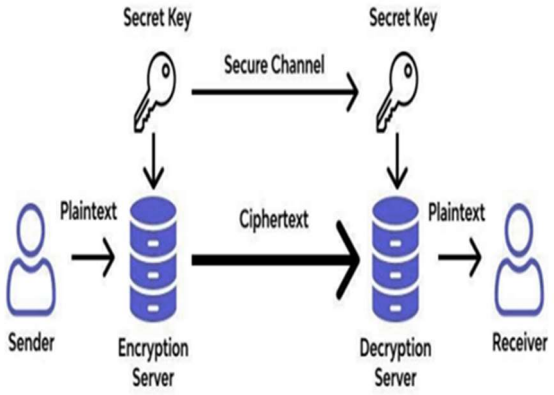

Figure 5. Framework model

STEPS FOR SECURE MESSAGING

The first and foremost is the user need to setup the touch Id in their respective devices. After that the device will authenticate by scanning the fingerprint.

Once the user enters the messing window the user would type their messages which will be encrypted and stored in the database. The receiver will view the authenticated or encrypted message by verifying their identity then finally the original message will be displayed to the receiver.

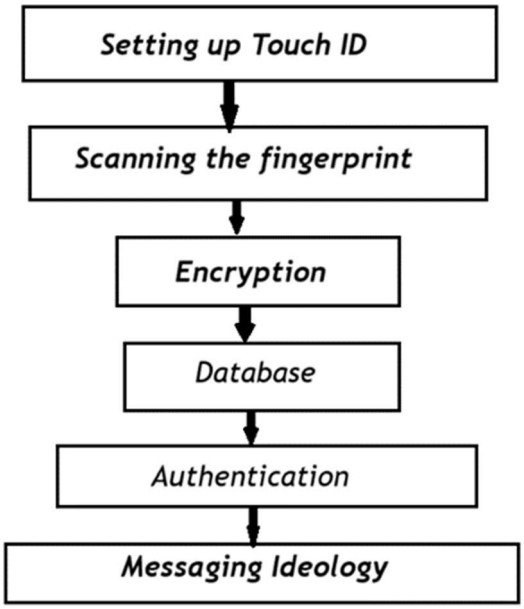

Figure 6. Steps for Secure Messaging

Configuring Touch ID: the individual needs to configure Touch ID on their gadget. This can usually be done in the software itself in a section designated for inserting authenticated user IDs.

Fingerprint scanning: The gadget will then scan the user's fingerprint using its fingerprint authentication. In order to verify whether that individual is the one wishing to begin the session, this is done.

Encryption: The user can type a message in the chat box after opening a chat window. When the transmit button is clicked, a socket for 31 is formed, allowing the sender and the recipient to communicate in both directions. The message is then encrypted and transferred to the database using the server medium and the sender's service provider.

Database: The user's mobile phone number will be listed in the database under the "USERS" collection. Additionally, a brand-new collection named "Chatroom" will be made, and it will contain a number of array-type documents that keeps the names of the sender and recipient. Additionally, it contains hierarchical collections that record fields like Send By, Time, and Encrypted Messages.

Authentication: The device will verify the user's identification and display the chat dashboard if the face or touch scan matches the data that has been stored. The user will be prompted to try again or select an alternative authentication method if the facial recognition is inconsistent with the stored data and the authentication fails.

Messaging Ideology: Through the search menu, users can look for and message other verified users. He or she will only be able to view the encrypted sender and recipient messages on the Message screen. An additional verification is required to view the original message. This

verification can be done using face or touch IDs, that will decode the message for a set amount of time, or by pressing the message for a long time, which will also decode the message till the user holds it.

This gives the user the highest level of privacy possible, preventing anybody else from seeing their messages.

ANALYSIS

Information is stored in plain text format in applications without encryption as well as access control mechanisms, making it readily readable and accessible to anybody who obtains access to it. All of the information retained by the application is accessible to everyone who has installed it. This may constitute a serious security issue, particularly if the software keeps private data, as everyone could be able to obtain this data if they had access to the device. On the other hand, apps that use high-level security features like encryption and access control mechanisms shield private data from theft or unwanted access by encrypting it so that only authorized users may decrypt and access it. In general, they are thought to be safer and a better option for keeping private data. Additionally, they provide more precise control over who has access to the data kept within the application.

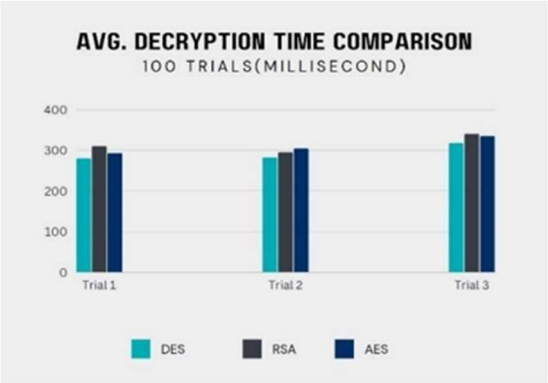

Figure 7. Average Decryption Time Comparison

The average decryption times of the DES, RSA, and AES algorithms are compared in figure. It demonstrates how quickly the AES algorithm can decode data. In the absence of these safeguards, apps save data in plain text, which makes it readily accessible to everyone who gets permission to the device. This could be a serious privacy issue, especially if the software keeps private data. Apps that employ access control and encryption, on the other hand, can shield private data against loss or illegal access.In conclusion, apps with restricted access and encoding are safer and more appropriate for keeping private data. They give a further line of defense against theft or unwanted access in addition to granular authority over who may access the data kept within the application.

CONCLUSION

It is advised to utilize AES encryption when combined with an access control mechanism in messenger applications to protect user confidentiality and safety. Effective security is provided via AES encryption, which is hard to crack, and sensitive information can be controlled with the application of an access control mechanism. Together, they can aid in preventing unwanted invasion of user data and guaranteeing the confidentiality of sensitive information. It is crucial to remember that although encryption adds an extra degree of security, it is not infallible and that other security flaws might also need to be fixed in order to guarantee the integrity of the messaging program. Furthermore, the efficacy of the mechanism for controlling access depends on how well it is managed and implemented, since a flawed setup or design may threaten system security. All things considered, implementing an AES-based access control system is a crucial step in creating a chat software that is safe and privacy-focused. Nonetheless, it ought to be a component of a more comprehensive security plan that incorporates continual risk evaluation and frequent changes to handle any potential fresh risks or vulnerabilities. AES's quick decryption performance makes it the clear winner when contrasted with other encryption techniques based on decryption time. AES uses a symmetric encryption key, which is one of the main factors contributing to its faster decoding performance.

This drastically cuts down on the amount of time required for decryption because the identical password is utilized to perform encryption and decryption. On the other hand, decryption is significantly slower with asymmetric encryption techniques like RSA since they utilize unique keys for encryption and decryption. AES can also fully utilize the processing capacity of modern central processing units since it is tailored for contemporary computer hardware. This indicates that massive volumes of data can be swiftly and effectively encrypted and decrypted with AES. In conclusion, given to its rapidity, effectiveness, and robust encryption capabilities, AES is the obvious choice when it involves encryption techniques based on decryption time.

REFERENCES

[1] S. Srinivasan, S. Sahoo, S. S. Raj, "Secure Sharing of Multimedia Content using Attribute-Based Encryption in Mobile Messenger Applications," IEEE Access, vol. 10, pp. 1289212907, 2022.

[2] H. Shang, W. Li, Z. Liu, H. Jin, "PrivacyPreserving Access Control for Cloud-Based Instant Messaging Services," IEEE Transactions on Dependable and Secure Computing, 2022.

[3] C. Kim, H. K. Lee, H. G. Kim, "Secure and User-Friendly Access Control for End-to-End Encrypted Instant Messaging," International Journal of Security and Networks, vol. 16, no. 2, pp. 128137, 2021.

[4] A. Ramamoorthy and P. Jayagowri, “A secure public key cryptosystem based medical records using non-commutative group”, Journal of Physics: Conference Series, Volume 1964, Advancesin Computational Mathematical Sciences, 2021.

[5] R.Gayathri, C.Kalieswari, “Multi-User Chat Application”, The International Journal of Engineering and Advanced Technology, Volume-9 Issue-5, PP: 372-374, June 2020.

[6] Diotra Henriyan, Devie Pratama Subiyanti, Rizki Fauzian, "Designing and deploying a real-time webbased chat server", International Conference on Engineering and Technology, 2016.

[7] Shabnam Bano and Mohd Atique, "Secure and Efficient Data Storage and Access in Cloud Using AES Encryption Algorithm", the International Journal of Computer Applications in Technology,2021.

[8] Saurabh Yadav and Ankit Jain,” Cloud Security using AES Encryption Algorithm", International Journal ,vol 13,2019.

[9] Dr.J.Akilandeswari, G.Sumathi,” Improved fuzzy weighted-iterative association rule based ontology post processing in data mining for query recommendation applications”, Computational Intelligence, Volume 36 , Issue 2,pp:1-10,Jan 2020.

[10] Karthikeyan, D. & Mohanraj, V. & Suresh, Y. & Senthilkumar, J.. (2020). “Hybrid Intrusion Detection System Security Enrichment Using Classifier Ensemble”,Journal of Computational and Theoretical Nanoscience.,Vol 17,No.1,PP 434-438,2020.

[11] M.Marimuthu, Dr.J.Akilandeswari,P R Chellaiah,” Identification of trustworthy cloud services: solution approaches and research directions to build an automated cloud broker”,Computing,Oct 2021.

[12] Fahrianto, F,” End-To-End Encryption on the Instant Messaging Application Based Android using AES Cryptography Algorithm to a Text Message”, 10th International Conference on Cyber and IT Service Management (CITSM), pp. 01- 06, (2022).

[13] Nhan Tam Dang,Sinh Van Nguyen,Ha Manh Tran , “Sharing secured data on peer-to-peer applications using attributebased encryption" International University-Vietnam National University of HCMC , vol. 5,Issue 4 (2021).

[14] Rachmat, N,” Performance analysis of 256-bit AES encryption algorithm on android smartphone”, In Journal of Physics: Conference Series IOP Publishing, Vol. 1196, No. 1, p. 012049, (2019).

[15] Ali, A. and Sagheer, A,” Design of secure chatting application with end to end encryption for android platform”, Iraqi Journal for Computers and Informatics, 43(1), pp.22-27,(2017).

[16] Lu, Z. and Mohamed, H,” A complex encryption system design implemented by AES”. Journal of Information Security, 12(2), pp.177-187, (2021).

[17] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, Allah Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing", Security and Communication Networks, vol. 2020, Article ID 8863345, 16 pages, 2020.

[18] Velagala, N., Maglaras, L., Ayres, N., Moschoyiannis, S. and Tassiulas, L.,"Enhancing Privacy of Online Chat Apps Utilising Secure Node End-to-End Encryption" (SNE2EE). IEEE Symposium on Computers and Communications (ISCC) (pp. 1-3), (2022).

[19] Karabey, I. and Akman, G., " A cryptographic approach for secure clientserver chat application using public key infrastructure" (PKI). 11th international conference for internet technology and secured transactions (ICITST) (pp. 442- 446), (2016).

[20] Wardhono, W.S., Priandani, N.D., Ananta, M.T., Brata, K.C. and Tolle, H.," End-to-End Privacy Protection for Facebook Mobile Chat based on AES with Multi-Layered MD5". Int. J. Interact. Mob. Technol., 12(1), pp.160-167, (2018).