International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Chat Application With End To End Encryption Using AES Algorithm

Mayuri Rathore[1], Kumkum Rathore[2], Riya Pawar[3], Chetna Dhote[4], Ms. Kanchan Narware

Abstract:
In today's digital era, communication through chat applications has become an integral part of everyday life. However, the increasing number of cyber threats and data breaches raises serious concerns about user privacy and message confidentiality. This research focuses on developing a secure chat application that provides end-to-end encryption to ensure that only the sender and receiver can read the messages. The proposed system is implemented using Android Studio, Firebase, and the AES encryption algorithm. The encryption process secures all messages before they are transmitted, preventing unauthorized access even if the database is compromised. The application also integrates Firebase Authentication for user login and real-time messaging using Firebase Realtime Database. The results show that the proposed model provides secure, fast, and reliable communication while maintaining data privacy and user confidentiality.

Keywords: Android Studio, Java, MongoDB, WebSocket, Nodejs, Expressjs.

INTRODUCTION:

In the modern era of digital communication, chat applications have become one of the most widely used means of exchanging information. From personal conversations to business communication, these applications allow users to send text, images, and multimedia instantly. However, with the increase in data transmission over the internet, ensuring message privacy and protecting user data from unauthorized access has become a major concern.

Traditional chat systems often store messages in plain text on servers, which makes them vulnerable to hacking, data leaks, and unauthorized surveillance. Therefore, it is essential to design a chat application that ensures complete message confidentiality and integrity. End-to-End Encryption (E2EE) is one of the most effective techniques to achieve this. It ensures that messages are encrypted on the sender's device and decrypted only on the receiver's device, making the data unreadable to anyone else — including the service provider or server administrators.

In this project, "Secure Chat Application using End-to-End Encryption," focuses on providing a private and secure communication environment. It is developed using Android Studio for the front end, Firebase for backend data storage and authentication, and the AES (Advanced Encryption Standard) algorithm for encrypting and decrypting messages. This combination of technologies ensures that the application not only provides real-time messaging but also protects user data from potential security threats.

This paper aims to present the design, implementation, and evaluation of the secure chat application. It demonstrates how end-to-end encryption enhances data security and ensures user privacy in real-time communication.

LITERATURE REVIEW:

Several research studies and existing applications have focused on improving the security and privacy of digital communication. This section reviews various approaches and technologies used in secure chat systems and how they have influenced the design of this project.

[1]. M. Marlinspike and T. Perrin, "The Signal Protocol," Open Whisper Systems,2016.

This paper introduces the Signal Protocol, a cryptographic framework designed for secure messaging. It provides end-to-end encryption and forward secrecy, meaning that even if one key is compromised,

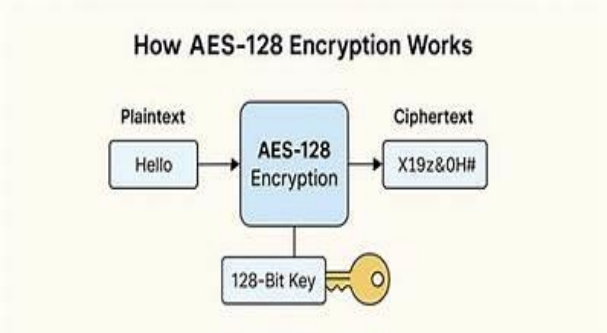
previous messages remain secure. The protocol has influenced many modern messaging apps, including WhatsApp and Facebook Messenger, due to its reliability and open-source nature.

[2]. W. Stallings, "Cryptography and Network Security: Principles and Practice,"7th Edition, Pearson Education, 2017.
This textbook provides a comprehensive foundation for understanding cryptographic techniques such as AES (Advanced Encryption Standard) and RSA. It explains how encryption ensures data confidentiality, authentication, and message integrity. The theories and algorithms discussed in this work serve as the theoretical backbone for secure communication systems like your chat application.

[3]. IARJSET, "Decentralised Chat Application with Enhanced Security," International Advanced Research Journal in Science, Engineering and Technology, Vol. 11, Issue 5, May 2024.
This paper proposes a blockchain-based decentralized chat system to improve security and privacy. By removing central data storage, it minimizes data breach risks. The research emphasizes peer-to-peer data transmission and encryption to achieve user-controlled communication. It inspired the concept of using encryption at user level rather than relying on centralized servers.

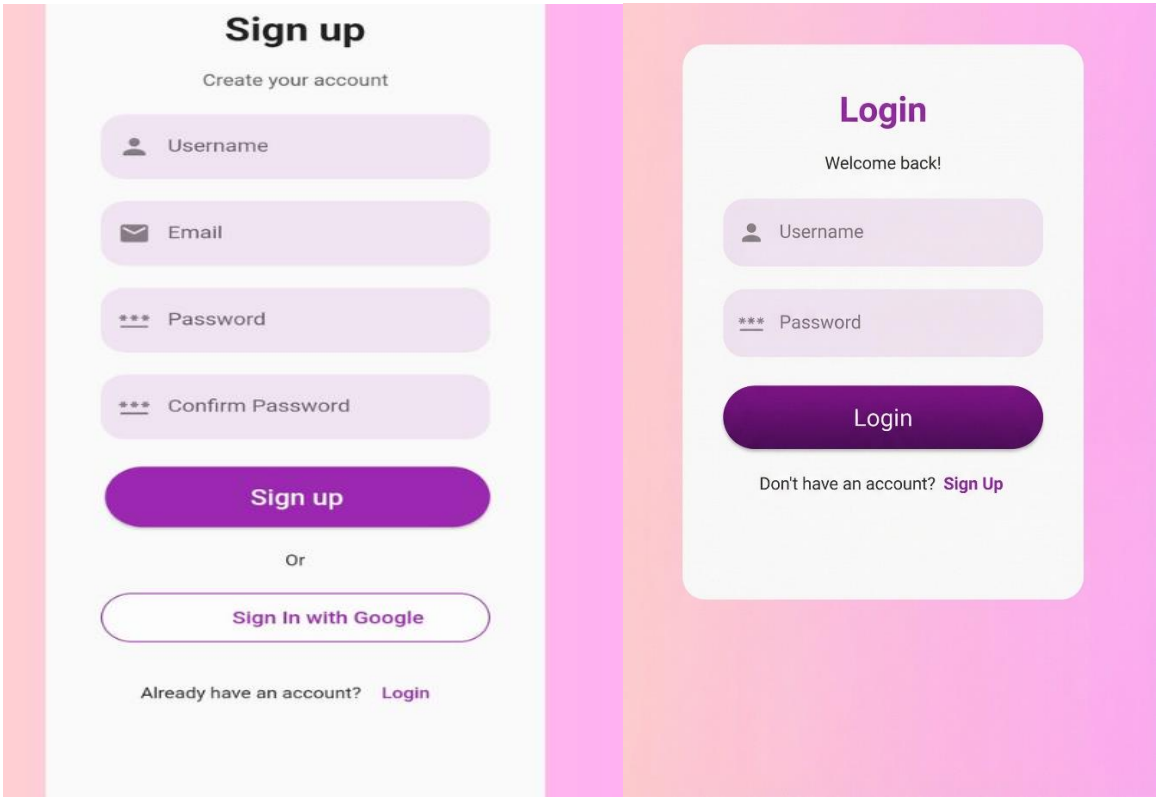
[4]. IIETA, "Secure End-to-End Chat Application: A Comprehensive Guide," International Information and Engineering Technology Association, 2024.
This study presents a detailed implementation of a chat system using end-to-end encryption for real-time messaging. It focuses on data confidentiality between sender and receiver and explains how symmetric key algorithms like AES can be applied efficiently in mobile applications.

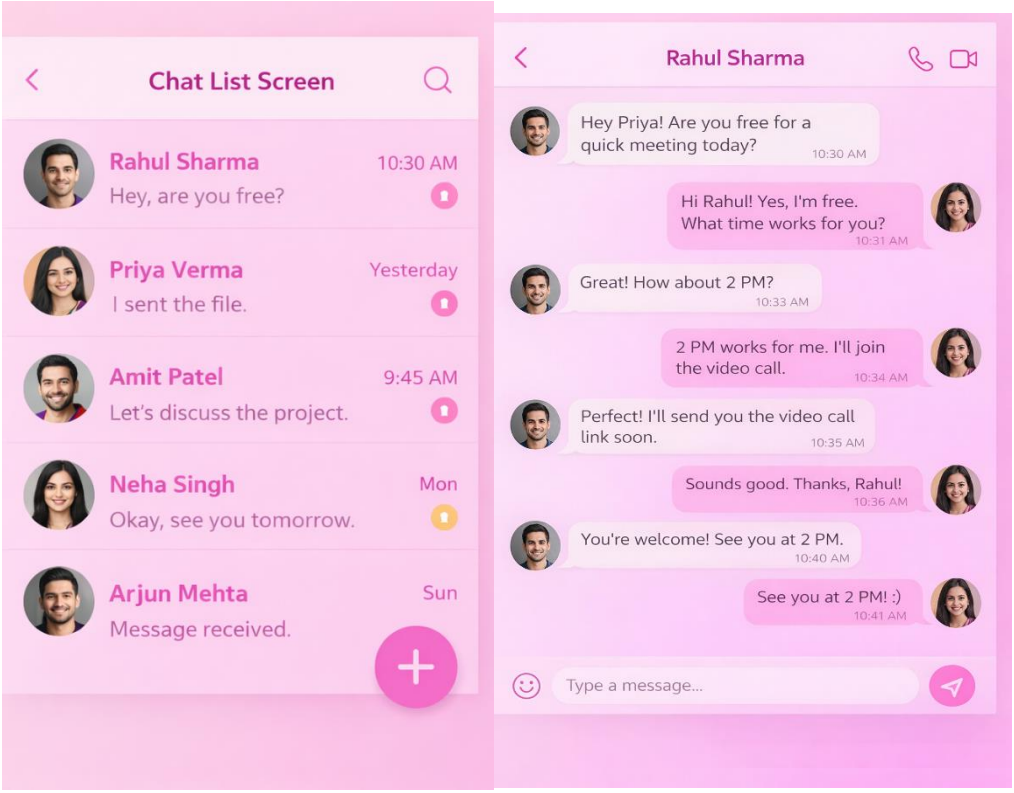
METHODOLOGY:
In this project The system uses the **AES (Advanced Encryption Standard)** algorithm to ensure secure communication between users in the chat application. AES is a symmetric key encryption technique, which means the same secret key is used for both encryption and decryption of messages. It was standardized and approved by the National Institute of Standards and Technology (NIST) in 2001 and is widely trusted for protecting sensitive digital information. In this project, the AES-128 variant is implemented because it provides strong security with a 128-bit key while maintaining high processing speed and low resource consumption, making it suitable for real-time mobile communication. When a user sends a message, the plaintext is encrypted into ciphertext using AES before being stored in the Firebase database. Even if unauthorized access occurs, the stored messages remain unreadable without the secret key. On the receiver's device, the same key is used to decrypt the ciphertext back into the original message. AES performs multiple rounds of substitution, permutation, and key mixing to ensure resistance against brute-force and cryptanalysis attacks. Due to its efficiency, reliability, and strong security model, AES is selected as the core encryption mechanism for implementing end-to-end encryption in this chat application.



RESULT:

In this project the Secure Chat Application was successfully implemented using Android Studio and MongoDB Realtime Database with AES-128 encryption. The results demonstrate that the system is capable of securely encrypting messages before transmission and decrypting them correctly at the receiver's end. During testing, all text messages were converted into encrypted ciphertext format before being stored in the database, ensuring data confidentiality and protection against unauthorized access. The application maintained smooth real-time communication with minimal delay, proving that AES encryption does not significantly affect performance on Android devices. Even when inspecting the MongoDB database, stored messages appeared in unreadable encrypted format, confirming that the encryption process works effectively. Only authenticated users with the correct secret key were able to decrypt and read the original messages. Overall, the system achieved secure, fast, and reliable end-to-end encrypted communication.





CONCLUSION

The "Secure Chat Application using End-to-End Encryption" successfully demonstrates how real-time communication can be made private, reliable, and secure by integrating encryption at the user level. The project ensures that only the sender and receiver can access the original message content, thus eliminating the risk of unauthorized access or data leakage.

By combining Android Studio, Firebase Realtime Database, Firebase Authentication, and the AES encryption algorithm, the application provides a complete solution for secure digital messaging. It maintains fast message delivery while ensuring confidentiality, integrity, and user trust.

This study highlights the importance of applying encryption not just at the server side but directly between users' devices. The results indicate that end-to-end encryption can be implemented efficiently even in lightweight mobile applications.

In the future, the system can be enhanced by adding multimedia encryption, group chat functionality, biometric authentication, and voice/video calling with secure transmission protocols. Such improvements would make the application even more robust and suitable for large-scale public use.

REFERENCES:

1. Payal Kshirsagar, Divyani Dhude, Dhanshree Sambare, Kanchan Narware: *"Implementation of Web based Online Chat Application"*, International Journal on Science & Technology, Vol 16(1), Jan-Mar 2025.
2. Mainka Saharan, Neeraj Kumar, Vijay Kumar, Akshay Juneja: *"Secure End-to-End Chat Application: A Comprehensive Guide"*, Review of Computer Engineering Studies, Vol 11(3), Sept 2024. DOI 10.18280/rces.110302.
3. Shashank Dabola, Vaibhav Tomer, Navpreet Singh, Dr. Parul Madan, Aryan Jhinkwan: *"Chat Secure-Messaging Application Based on Secure Encryption Algorithm"*, IJRASET, Volume 12(III), March 2024. DOI 10.22214/ijraset.2024.58817.

4. Dr Lokesh S, Canavero W M, Abhimanyu Dwibedi, Ajith B S, Anand Kumar, Neeharika Thangamma: *"Decentralised Chat Application with Enhanced Security"*,IARJSET,DOI10.17148/IARJSET.2024.11545.
5. Yang J., Chen Y.–L., Por L.Y., Ku C.S.: *"A Systematic Literature Review of Information Security in Chatbots"*, Applied Sciences, Vol 13(11):6355, 2023. DOI10.3390/app1311635
6. Prof. Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali: *"Survey Paper on Communication System Using Blockchain and Cryptography"*, IJRASET, May 2022. DOI 10.22214/ijraset.2022.42442
7. Christian Johansen, Aulon Mujaj, Hamed Arshad, Josef Noll: *"The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications"*, arXiv pre-print, July 2018.
8. Mohamad Andee Mohamed, Abdullah Muhammed, Mustafa Man: *"A Secure Chat Application Based on Pure Peer-to-Peer Architecture"*, Journal of Computer Science, Vol 11(5):723-729, 2015. DOI 10.3844/jcssp.2015.723.729.