International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Chat Application With End To End Encryption Using AES Algorithm

Mayuri Rathore[1], Kumkum Rathore[2], Riya Pawar[3], Chetna Dhote[4], Prof. Satish Chadhokar[5]

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.

The proposed 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.

SCOPE OF THE STUDY:

The scope of this project is to design and develop a secure chat application that ensures private communication between users through end-to-end encryption. The application focuses on providing a safe and user-friendly platform for exchanging text messages in real time.

The study is limited to implementing text-based communication using the AES encryption algorithm in combination with Firebase Realtime Database for message storage and synchronization. The Firebase Authentication service is used to manage user login and registration securely.
This research primarily targets Android mobile users, offering a lightweight and efficient messaging experience without compromising data security. While the current version focuses on one-to-one communication, the scope can be extended in the future to include group chats, multimedia message encryption (images, videos, audio), and integration of additional features such as message deletion, notifications, and biometric authentication for enhanced privacy.

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]. 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.Presents design and implementation of a real-time web-based chat system emphasizing usability, instant communication, and security measures for efficient user interaction.
[2]. Mainka Saharan, Neeraj Kumar, Vijay Kumar, Akshay Juneja: *"Secure End-to-End Chat Application: A Comprehensive Guide"*, Review of Computer Engineering Studies,Vol11(3), Sept 2024. DOI 10.18280/rces.110302.Explains complete architecture and working of secure chat applications using end-to-end encryption to ensure data confidentiality, integrity, and user authentication**.**
[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. Focuses on developing a secure messaging app implementing modern encryption algorithms to protect message content and user privacy from unauthorized access.
[4]. Dr Lokesh S, Canavero W M, Abhimanyu Dwibedi, Ajith B S, Anand Kumar, Neeharika Thangamma: *"Decentralised Chat Application with EnhancedSecurity"*,IARJSET,DOI10.17148/IARJSET.2024.11545. Proposes a blockchain-based decentralized chat model ensuring user data privacy, transparency, and resistance to single-point failures through distributed communication.
[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/app13116355. Analyses existing research on chatbot communication security, identifying vulnerabilities and proposing secure frameworks to enhance data protection in chat systems.
[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. Surveys blockchain and cryptography techniques applied in secure communication systems, highlighting their potential for protecting chat applications and user identities.
[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. Compares popular secure messaging apps, evaluating encryption methods, privacy policies, and performance to identify strengths and weaknesses of current solutions.
[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. Introduces a peer-to-peer chat system eliminating centralized servers, enhancing communication privacy and reliability through direct encrypted connections between users.

Proposed Methodology:

The proposed system uses the AES (Advanced Encryption Standard) algorithm to ensure secure communication between users. AES is a symmetric key encryption algorithm, which means the same key is used for both encryption and decryption of messages. It is one of the most reliable and efficient encryption algorithms used in modern applications and is approved by the U.S. National Institute of Standards and Technology (NIST).

In modern communication systems, encryption plays a crucial role in securing data transmission. Various symmetric and asymmetric algorithms are available, including DES (Data Encryption Standard), Triple DES (3DES), RSA (Rivest–Shamir–Adleman), and AES (Advanced Encryption Standard). Each has its own strengths and limitations depending on the desired balance between speed, security, and computational efficiency.

The DES algorithm, though historically significant, is now considered insecure due to its short 56-bit key length, which makes it vulnerable to brute-force attacks. Triple DES (3DES) improves upon DES by applying the encryption process three times, enhancing security but resulting in slower performance, making it less suitable for mobile or real-time applications. RSA, an asymmetric encryption method, offers robust security through public and private key mechanisms; however, it requires significantly higher computational power and processing time, which reduces its efficiency for real-time chat systems.

In comparison, AES (Advanced Encryption Standard) provides an optimal balance of security, speed, and resource efficiency. It supports multiple key lengths (128, 192, and 256 bits) and performs multiple rounds of substitution, permutation, and key mixing, making it highly resistant to brute-force and cryptanalysis attacks. The AES-128 variant, used in this project, ensures strong encryption with minimal latency, which is ideal for mobile-based chat applications. Unlike RSA, it performs faster due to its symmetric key nature and consumes less battery and processing power.

Therefore, AES is identified as the most suitable encryption algorithm for secure chat applications that require real-time communication, high performance, and strong data confidentiality. Its widespread adoption, proven security model, and compatibility with Android platforms make it the preferred choice for implementing end-to-end encrypted messaging systems.

RESEARCH GAP

While several existing chat applications, such as WhatsApp, Telegram, and Signal, use advanced encryption protocols to secure communication, there are still some limitations and research gaps that this study aims to address:

Although several secure chat applications and encryption frameworks exist today, there remain significant gaps in terms of accessibility, transparency, and adaptability for small-scale developers. Most existing systems are heavily dependent on centralized servers, which increases the risk of server-side attacks, unauthorized access, and potential data leaks if proper end-to-end encryption is not enforced. Additionally, some widely used encryption protocols such as MTProto (used by Telegram) or Signal Protocol (used by WhatsApp) are proprietary and not fully open for academic evaluation, limiting opportunities for independent testing, verification, and improvement.

Another major limitation is the lack of lightweight and beginner-friendly secure frameworks. Many existing solutions are complex, resource-intensive, and difficult for students or small developers to understand and implement. There is a clear need for a simple yet secure model that integrates easily with platforms like Firebase, providing both efficiency and security. Furthermore, most research and implementations focus solely on text message encryption, overlooking the need for securing multimedia data such as images, audio, and video, which are essential components of modern chat systems.

Lastly, user authentication and identity verification mechanisms in many existing models remain inadequate, making them susceptible to impersonation or unauthorized account access. Addressing these gaps, this research introduces a Firebase-based chat application employing AES encryption and Firebase

Authentication to create a secure, transparent, and easy-to-implement solution for real-time 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/app13116355. 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
6. 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.
7. 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.