International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Real Time Chat Application With End-to-End Encryption

Devang Mani Tripathi
Ismail Khan
Simarpreet Singh
Department of Computer Science and Engineering
Galgotias University, Noida, India

***Abstract*—The extensive spread of digital communication technologies has made real-time chat applications an essential part of the modern world. The wide use of these applications is in the fields of personal correspondence, team collaboration, education, healthcare provision, and business activities. However, the growing dependence on the centrally operated server-based communication systems has created strong concerns in regard to the confidentiality of the data, privacy of message, and security of the users. Cyber-attacks, clandestine monitoring, identity theft, and massive data leaks have been progressively frequent and thus user sensitive data is exposed to more risk. Traditional messaging systems normally store user messages on centrally positioned cloud environments, hence, becoming an appetizing target to malicious entities. In a situation where encryption systems have been installed, the service providers can have access privileges to data, thus undermining the privacy of individuals. The vulnerabilities have provoked a desperate need to establish safe communication infrastructures that can enable the end users to have a full control of data. Regarding the above exigencies, this manuscript outlines the conceptualisation and implementation of a secure real-time chat system based on end-to-end encryption (E2EE). The architecture guarantees that the communicating parties have decryptive abilities only by encrypting messages locally on the device of the sender and decrypting them only on the device of the recipient. As a result, the server or service provider has no right to read transmitted material or any other ancillary party. The system implements the AES, version 256, to protect the payload, uses RSA to engage in key negotiations, implements Firebase Authentication to identify who a user is, and uses Firebase Realtime Database to facilitate the exchange of encrypted messages.**

The architecture proposed creates confidentiality, integrity and authenticity and still maintains the sub-latency measures of performance. Experimental evaluations attest to the fact that the solution enables fast and reliable real-time communication at a low cost of computation. The results support the claim that well-developed cryptographic schemes can easily be incorporated into the real-time messaging infrastructure without affecting the usability or user experience.

***Index Terms*—Secure Chat Application, End-to-End Encryption, AES, Firebase, Cyber Security, Data Privacy**

I. CHAPTER I: INTRODUCTION

The rapid development of internet technologies, mobile computing and the cloud-based services has clearly altered the way that inter-personal communication is carried out within the digital epoch. Instant messaging applications have become essential channels for exchanging textual, visual and multimedia content in real time over disparate geographic loci.

The current digitalisation of public and private services has contributed to the increasing use of chat platforms in areas such as education, healthcare, commerce, banking and government communication. Sensitive information - from personal information and financial information to medical records and proprietary corporate documents - is increasingly transmitted over these mediums. Consequently, the need to protect privacy and guarantee security of communication via electronics has become an imperative.

Recent years have seen a sudden spread of cyber threats, such as man-in-the-middle attacks, phishing attacks, identity theft, clandestine surveillance and database breaches. These negatively not only compromise user privacy but also affect the trust of users towards the digital communication infrastructures, making people more vigilant when it comes to secure communication systems that can defend their personal and professional information from unauthorised access.

End -to -end encryption (E2EE) has become a dominant solution to meet such security requirements. In a structure that uses E2EE data, messages are encrypted on the sending device and are decrypted on the receiving device only, meaning that any intercepted data cannot be made comprehensible to unauthorised entities, even if they are sent or stored on third-party servers.

This work focuses on the design and implementation of a secure, real-time chat application, which combines end-to-end encryption with powerful authentication and encrypted storage in the cloud. The proposed system aims to provide a reliable, private and user-friendly communication platform that meets modern security needs while maintaining the high performance and usability.

II. CHAPTER II: LITERATURE REVIEW

Secure digital communication is a major area of research due to the increasing number of cyber threats and privacy concerns related to the latest messaging platforms. Numerous investigations have attempted to come up with secure chat ecosystems using cryptographic techniques, distributed structures and privacy-preserving mechanisms.

Early messaging infrastructures mainly used transport layer security protocols such as SSL and TLS to provide protection for data in transit. Whilst these methods reduce an attack at network level, there are no ways to prevent service providers

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

to access the content in the messages, thereby, user privacy is also vulnerable to internal data breaches and unauthorized surveillance.

A number of researchers have proposed secure chat solutions that incorporate cryptographic primitives such as AES, RSA and Elliptic Curve Cryptography (ECC). AES is preferred for its high throughput and strict security properties, making it suitable for real-time communication systems. RSA and ECC are used for secure key exchange and digital signature generation on a regular basis, ensuring message authenticity and integrity.

Contemporary messaging platforms that are secure - including WhatsApp, Signal, Telegram, and Viber - have made their messaging more or less encrypted. However, their security models differ and not all applications provide default end-2-end encryption. Moreover, a dominance of proprietary, closed source designs makes independent security audits difficult.

The literature highlights the need to note considerable advance made in the evolution of secure communication systems, although there remain several challenges. Centralised storage of data, lack of transparency, service provider dependency, and lack of end-to-end encryption implementation are among the factors that demonstrate the need for a transparent, secure and developer-friendly chat application that gives end users the choice to control their data.

A. Analysis of Existing Messaging Applications

This section provides a brief look at some of the main messaging applications, their security and privacy features.

1) Viber: Viber is the most deployed instant messaging and the Voice over the IP (VoIP) platform, which allows exchanging text messages, images, videos, and audio. While Viber claims to be an option for encrypted communication, there are still limitations, especially when it comes to attachments sent via third-party applications like iOS share extensions.

2) WhatsApp: WhatsApp is one of the most common messaging platforms in the world with billions of active users. It has end-to-end encryption through the Signal protocol so that only the sender and the receiver can access message contents. Nonetheless, metadata, such as contact information, timestamps and data that are stored in the cloud for backup reasons, may be accessible to service providers, raising ancillary privacy issues.

3) Telegram: Telegram provides two forms of messaging: traditional cloud-based messaging chats and secret chats. Standard chats are cloud hosted, and don't have end-to-end encryption, allowing the Telegram servers to store and sync messages across devices. This bifurcated architecture gives rise to confusion about actual message security on the part of users.

4) Facebook Messenger: Facebook messenger offers an optional secret conversation mode that is end-to-end encrypted. However, ordinary chats are stored on the servers of Facebook and are available to Facebook company. As secret conversations are not enabled by default, most users go on talking unencrypted without awareness of the associated security implications.

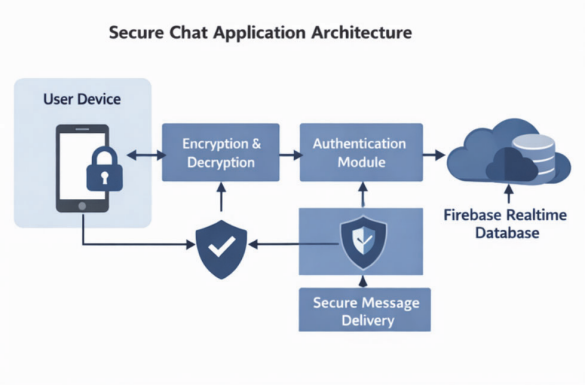

Fig. 1. System Architecture

B. Research Gaps

Analysis of the existing literature and the study of existing messaging platforms highlight the following research gaps:

Especially default end-to-end encryption for all users is eschewed by the majority of applications. * Centralised server architectures store user data mostly. * Proprietary implementations make it difficult to verify security independently. * Metadata leakage remains a serious privacy liability. * Users are limited in their authority over encryption keys and data repositories.

These lacunae highlight the need to have a secure, transparent and user centre chat application that ensures absolute privacy with true end-to-end encryption, robust authentication and encrypted cloud storage.

III. CHAPTER III: SYSTEM ARCHITECTURE

The proposed secure chat application is developed based on a client-server architecture that is integrated with E2EE (end-to-end encryption). This architecture ensures that the message content is kept secret and is not accessible to unauthorised users (including the service provider).

The architecture of the overall system is divided into five major components, namely the client interface, authentication module, encryption engine, database server, and message delivery system. Each component has a critical role to play in ensuring secure, reliable and real-time communication between users.

A. Client Interface

It is designed to be simple, intuitive and user-friendly at the same time as having strong security mechanisms in the background. The interface enables the user to register, login, send messages, receive messages, and manage the conversations. The client application also provides for safeguarding encryption keys and decryption is only done after receiving the encrypted messages from the server.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

B. Authentication Module

This module ensures that only authenticated users could access chat application. It also helps to prevent impersonation, unauthorized login and misuse of accounts. By adding a trusted authentication framework, the system to promote greater trust from users and reliability of the platform.

C. Encryption Engine

Encryption engine is the primary security component of the system. It is responsible for the encryption of all outgoing messages and decryption of incoming messages. The reason for the use of the Advanced Encryption Standard (AES-256) algorithm to encrypt the message content is its strong security guarantees and high performance.

Secure mechanisms for key exchange are provided to exchange the encryption keys between users who communicate with each other. To avoid key reuse and minimize the risk of cryptographic attacks, each communication session has a unique encryption key. The encryption engine can also support the use of digital signatures to provide authentication and integrity of the message.

D. Database Server

Firebase Realtime Database is used as a backend storage system for encrypted messages. The server only stores encrypted message data and is never processing or storing plaintext information. This way, even if the database gets hacked, the hackers cannot read the message contents.

The database offers a means of real-time synchronization, and messages can therefore be delivered immediately to the online user. It also supports offline message storage which ensures that messages are delivered once the receiver becomes active.

E. Message Delivery System

Firebase cloud messaging (FCM) is used to deliver messages for push notifications and ensure instant delivery of messages.

It makes sure that the users receive messages on time, even if the application is running in the background. This component has a crucial role in keeping the chat application responsive and in real time.

IV. CHAPTER IV: METHODOLOGY

This chapter explains methodological framework and method taken in the development of secure real-time chat application. The methodology is focused on strong security measure, reliability and high performance with an user-friendly interface. The system architecture is then modular, where each component is responsible for a different function such as authentication, encryption, message transmission, and data storage.

The main goal of the methodology is to ensure that user messages are confidential and secure from unauthorised access at any point in the communication process, creating messages, encrypting them, transmitting them, storing them and decrypting them.

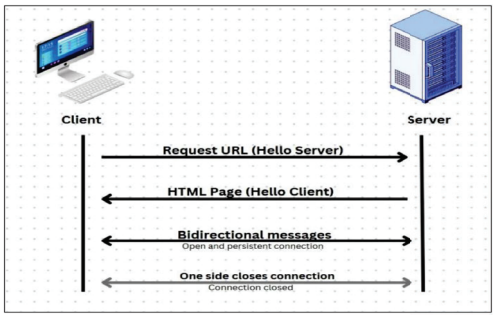

Fig. 2. Message Flow- Diagram

A. System Workflow

The general working of the system has been described in the following steps:

1) The user installs the application and creates an account by providing the valid email address and password.
2) Firebase Authentication verifies the credentials of the user and grants access to the application.
3) When the user types a message and transmits it, the message goes through the encryption engine first.
4) The plaintext message is encrypted using the AES-256 encryption algorithm before it leaves the sender's device.
5) The encrypted message is sent safely through the servers of Firebase.
6) When the encrypted message is received by the receiver's device, it is decrypted using the same key which was shared between the two devices.
7) The message after decryption is shown to the user in the chat interface.
8) Messages are also stored locally on the device in encrypted form to ensure offline access with security.

B. Cryptographic Techniques Used

The security of the proposed chat application is based on well-known and used cryptographic standards. Multiple cryptographic methods are used to provide confidentiality, integrity and authentication.

1) AES Encryption: Advanced Encryption Standard (AES-256) that is used to encrypt message content AES is a symmetric encryption algorithm which has been given a large amount of trust and used in many different secure systems. It has a high level of security and it has expedited encryption and decryption speeds, which makes it suitable for real-time communication environments. Each communication session has a unique AES key so that keys are not reused and the potential for cryptographic attacks is reduced.

2) RSA Key Exchange: RSA is being utilised for this purpose of secure key exchange between users. Every user is provided a public-private key combination. Only the recipient can decrypt this AES key with the recipient's private RSA key and thereby make the key distribution secure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

3) Digital Signatures: Digital signatures have been implemented to check the authenticity and integrity of the messages. Before transmission, the message is signed with the sender's private RSA key along with a cryptogram of the message. The receiver will validate the signature by using the sender public key. This procedure ensures that the message has not been modified on the way, and establishes the identity of the sender.

C. Design Considerations

Several major design considerations had an impact on how the system was developed. The application was designed to be light and efficient in order to work smoothly on a wide range of Android devices. Particular emphasis has been placed on minimising the consumption of batteries and the network.

Scalability was also a critical factor while designing the Firebase services were chosen because of their ability to handle large numbers of concurrent users and support real-time data syncing. Consequently, the system is able to support a growing user base without compromising performance.

All in all, the methodology ensures that the chat application under consideration provides a secure, reliable, and high-performance communication platform while maintaining ease of use and accessibility for end users.

V. CHAPTER V: SECURITY ANALYSIS

The basic groundwork of the proposed real-time chat application is security. The system has been carefully designed to ensure user data is protected at every step in the communication process, including the creation of messages, encryption, transmission, storage, and decryption. Multiple levels of security mechanisms have been established to ensure confidentiality, integrity, authentication and resilience to common cyber threats.

The security model follows the principle of "zero trust," which means that no part of the system is trusted by default. All sensitive operations run on the client side, and the server is reduced only to the level of message relay and encrypted data storage service.

A. Confidentiality

Confidentiality requires the information contained in the message to be accessible only to the intended sender and receiver. In the proposed system all messages are encrypted using the AES-256 algorithm before they are transmitted over the network. Since encryption is being done on the sender's device, plaintext data is never exposed to the network or the server.

Even if an adversary was to intercept the communication channel or gain access to the server database, the ciphertext will be unintelligible without the decryption keys. This methodology provides for absolute privacy of conversations between users and inhibits unauthorized surveillance.

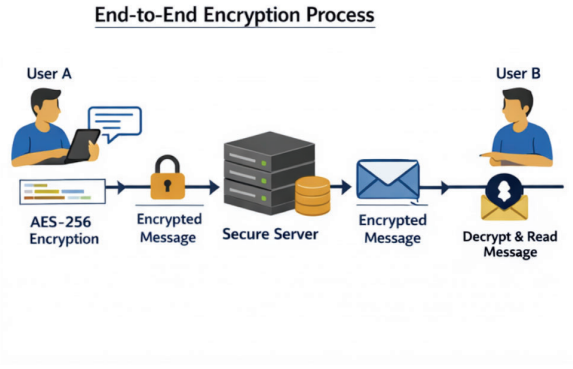

Fig. 3. End-to-End Encryption Process

B. Integrity

Integrity is a guarantee that messages are not altered or tampered with during transmission. The system uses cryptographic hashing and digital signatures to check the integrity of messages. Each message is signed by the sender with a private key, which the receiver uses to validate the signature using the public key of the sender.

Should any alteration occur during transmission of the message through the network, the integrity verification process will fail and thus provide an alert to the receiver. This mechanism prevents attackers from injecting malicious content or making changes to legitimate transmissions.

C. Authentication

The authentication ensures that only the legitimate users will access the chat system. Firebase Authentication is used to authenticate users when they register and login, thereby preventing users from creating false accounts or impersonating as other users.

Apart from these, cryptographic identity verification plays a role in secure communication sessions. Each user has his or her own public-private key pair which creates trust between communicating parties.

D. Server Protection

The server is designed purposefully to be only a message relay and encrypted data storage platform. It never processes/retains plaintext messages. All data stored in the Firebase Realtime Database is always encrypted, and encryption keys are never shared with the server.

As a result, even in the event of a compromise of the server infrastructure, attackers are unable to access readable message content. The server does not have any technical capability of decrypting messages and thus guarantees the true end-to-end encryption.

E. Attack Resistance

The proposed system is built to resist a wide range of common cyber -attacks, including:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- **Man -.in -the- middle attacks:** Secure key exchange and digital signatures make it difficult for adversaries to intercept and modify communications.
- **Data interception:** Encrypted data packets are unintelligible even if data traffic is intercepted.
- **Unauthorized database access:** Encrypted storage means that exfiltrated data cannot be decrypted.
- **Replay attacks:** Unique session keys and message timestamps prevent the re-transmission of old messages.
- **Impersonation attacks:** Strong authentication and cryptographic identity verification make impersonation attacks impossible.

Overall, the security architecture ensures the proposed chat application offers a robust and trustworthy communication platform. Being a combination of powerful encryption, secure authentication, encrypted cloud storage, and attack-resistant protocols, the system offers a high level of security suitable for the modern digital communication environments of today.

VI. CHAPTER VII: RESULTS AND DISCUSSION

The experimental evaluation of the proposed secure real-time chat application shows that the system is able to successfully meet its main goals of security, performance, and usability. The application was tested under different network conditions and configurations of devices to assess the feasibility and reliability of the application in real life.

The results show that the integration of end-to-end encryption does not cause apparent delays in message transmission. Messages are delivered in real time with little latency even if the encryption and decryption operations are on the client side. This validates that it is possible to achieve strong cryptographic security without sacrificing the user experience.

The encryption and decryption processes were calculated to be computationally efficient and therefore the system should be suitable for use continuously in mobile devices. Battery consumption and data usage were kept to acceptable levels, an important factor for mobile users who rely on chat applications to communicate with peers on a daily basis.

From the perspective of security the system successfully blocked access to the content of messages from unauthorized parties. Encrypted messages stored at the server were not readable without the corresponding decryption keys, and thus completely private.

Overall, the experimental results confirm that the proposed system offers a secure, fast and reliable communication platform. The balance that is made between the strong security mechanisms and the high system performance make the application suitable for deployment in real-world environments where privacy and data protection are critical requirements.

VII. CHAPTER VIII: APPLICATIONS

The secure real-time chat application proposed in this paper can be successfully applied in a wide range of domains where confidentiality, privacy and data security are basic requirements. In an age of increasing dependence in the use of digital communication platforms, organisations and individuals

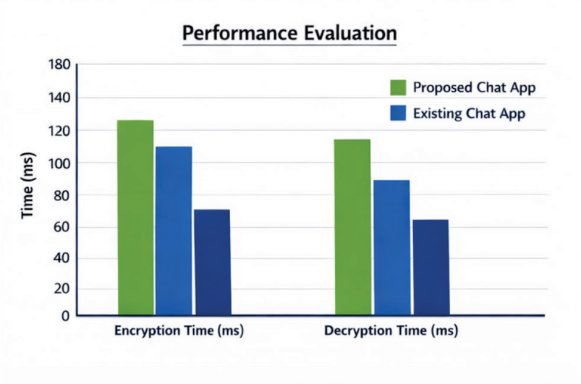

Fig. 4. Performance Evolution

Comparison of Messaging Apps

Feature	WhatsApp	Telegram	Signal	Viber
End-to-End Encryption	Yes	Yes	Yes	Optional
Open Source	No	Yes	Yes	No
Cloud Backup Access	Yes	No	Yes	No
Metadata Protection	Limited	High	Yes	Limited

Fig. 5. Comparison Of Apps

alike are demanding robust systems that can protect sensitive information from unauthorised access and cyber threats.

One of the main uses of the proposed system is in **personal communication**. Individuals may use the platform to communicate in private messages with family members and acquaintances and transfer private information, photographs, and confidential data while reducing concerns about surveillance, data leakage or unauthorised intrusion.

Within the sphere of **business and corporate communication** the application allows secure inner correspondence between employees, management and outside partners.

In **educational institutions** the system is used for confident communication between students, faculty and administrative personnel. Crucial academic documents, examination information and protected student records can be shared securely via the platform.

VIII. CHAPTER IX: CONCLUSION

This manuscript describes the design and implementation of a secure real time chat application that includes end-to-end encryption to protect user communication against unauthorised access and cyber threats. The system solves the growing problems related to the privacy of data, message confidentiality, and security of users in current digital communication systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

By combining AES-256 encryption to protect messages, RSA-based secure key exchange, authentication using the built-in Firebase Authentication service, the system ensures that only the intended sender and recipient can access the message content. The server is purely a relay and encrypted storage device without any ability to read or process clear text data thus providing true end-to-end encryption.

IX. CHAPTER X: FUTURE SCOPE

Although the real-time chat application has achieved the privacy, security and performance objectives, there are several opportunities for enhancing it in the future. As the digital communication is still evolving, new requirements and technology advancements can be integrated to make this system more powerful, scalable and feature rich.

One of the features that stand out as an improvement in the future is the addition of **encrypted group chat functionality**. This would allow multiple users to have a secure conversation, and be sure that all messages are protected through end-to-end encryption. Group key management methods can be applied to ensure confidentiality within large group discussions.

In conclusion, the scope of the potential future application of the proposed system is wide and promising. Continuous development and integration of emerging technologies will help the application to grow into a next generation secure communication platform offering complete privacy, high security and new functionality across different domains.

ACKNOWLEDGMENT

The author thanks the Department of Computer Science and Engineering, Galgotias University, for their support and guidance.

REFERENCES

[1] A. S. Bais et al., “Secure Chat Using Encryption,” International Journal of Research Publication and Reviews, vol. 6, no. 4, pp. 16487–16489, 2025.
[2] M. Rathore et al., “Chat Application with End-to-End Encryption Using AES Algorithm,” International Journal of Technology and Applied Science, vol. 16, no. 11, 2025.
[3] S. Surendar Raj and K. Sai Varsha, “Developing an End-to-End Secure Chat Application,” International Journal of Scientific Research & Engineering Trends, vol. 11, no. 6, 2025.
[4] C. Johansen et al., “The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications,” arXiv preprint, 2018.
[5] Fette, I., Melnikov, A. (2011). The WebSocket Protocol. RFC 6455, IETF.
[6] Fielding, R. T., Taylor, R. N. (2000). Architectural styles and the design of network based software architectures. Doctoral dissertation, University of California, Irvine.
[7] Banks, A., Porcello, E. (2017). Learning React: Functional Web Development with React and Redux. O’Reilly Media, Inc
[8] C. Johansen et al., “The Snowden Phone: A Comparative Survey of Secure Instant Messaging Mobile Applications,” arXiv preprint, 2018.
[9] Express.js Documentation. (n.d.). Retrieved from https://expressjs.com/en/4x/api.html .
[10] MongoDB Documentation. (n.d.). Retrieved from https://docs. mongodb.com/
[11] Zustand Documentation. (n.d.). Retrieved from https://github. com/pmndrs/zustand
[12] Daisy UI Documentation. (n.d.). Retrieved from https://daisyui. com/docs/
[13] OWASP. (2021). OWASP Top Ten. Retrieved from https://owasp. org/Top10