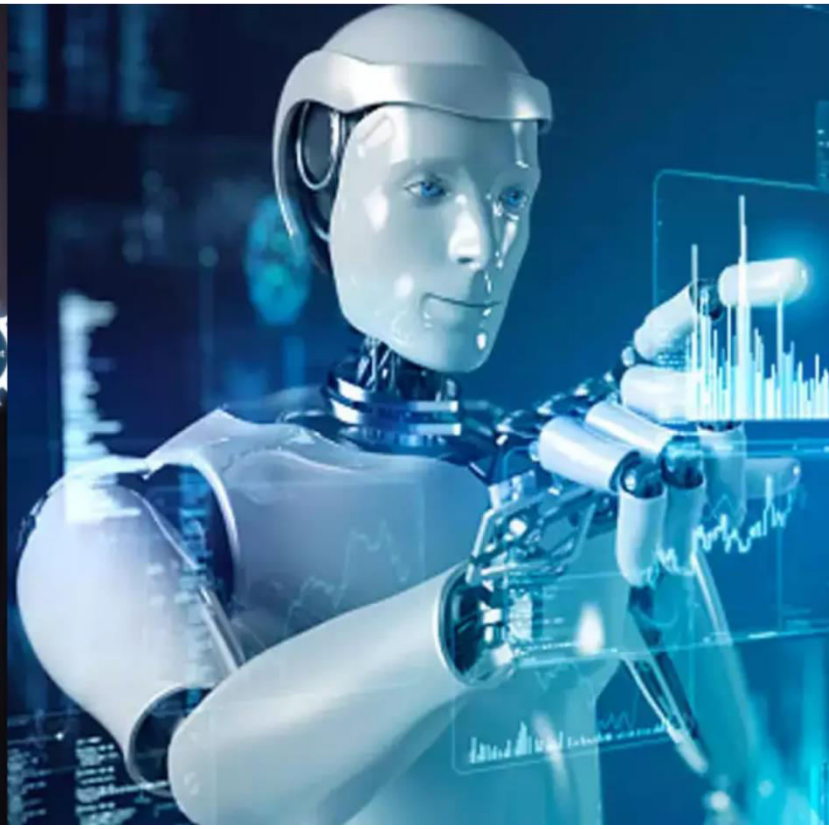
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 2, February 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

Secure Chat App with End-To-End Encryption

Devika S.P, Gayathri Devi G.S, Jenifer Shanu S

Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Nagercoil, Tamil Nadu, India

ABSTRACT: Modern communication depends heavily on instant-messaging platforms, yet user privacy is constantly threatened by data interception and unauthorized access. This project titled "Secure Chat Application with End-to-End Encryption" focuses on building a real-time chat system that guarantees confidentiality, integrity, and authenticity of messages through advanced cryptographic protocols. The system integrates Extended Triple Diffie-Hellman (X3DH) for session establishment, Double Ratchet Algorithm for continuous key evolution, and the DenIM (Deterministic Encrypted Metadata) layer for metadata protection. Group messaging is secured using the Messaging Layer Security (MLS) framework. These combined techniques ensure forward and backward secrecy while preventing even the server from reading user messages. Beyond algorithmic design, this report discusses the importance of encryption in widely used applications like Signal and WhatsApp, the need for metadata-free communication, and practical steps for user verification through QR codes and safety numbers. The proposed solution demonstrates how a well-implemented end-to-end encryption model can deliver a scalable and privacy-preserving chat platform suitable for both individual and enterprise communication.

KEYWORDS: End-to-End Encryption, X3DH, Double Ratchet, DenIM, MLS, Secure Messaging.

I. INTRODUCTION

Communication security has become one of the most critical challenges of the digital age. With billions of users relying on chat applications such as WhatsApp, Signal, and Telegram, the need for end-to-end encryption (E2EE) has grown exponentially. Traditional client–server models store message content on servers, exposing user data to potential breaches and surveillance. This project aims to design a Secure Chat Application that uses a hybrid cryptographic approach to ensure confidentiality, authenticity, and metadata protection. The application ensures that only the sender and receiver can read the transmitted messages—no intermediate server, ISP, or third party has access.

With the rapid growth of internet-based communication, instant messaging applications have become an integral part of daily life. These platforms enable real-time communication across geographical boundaries and are widely used for personal, educational, and professional interactions. However, the increasing dependence on digital communication has also raised serious concerns regarding data privacy, message confidentiality, and unauthorized access to sensitive information.

Traditional messaging systems rely heavily on centralized servers to manage message delivery and user authentication. Although many applications claim to provide encrypted communication, in practice, a significant amount of user data and metadata remains exposed to service providers. Metadata such as sender and receiver identities, message timestamps, communication frequency, and group membership can be exploited to infer user behavior patterns, even when message content is encrypted.

End-to-end encryption (E2EE) has emerged as a promising solution to address these security challenges. In an E2EE-based system, cryptographic keys are generated and managed exclusively by the communicating users, ensuring that only the intended recipients can access the plaintext messages. However, implementing secure E2EE alone is insufficient, as modern threat models also require protection against metadata leakage, key compromise, and unauthorized group access.

This paper proposes a secure chat application that integrates multiple cryptographic techniques to ensure confidentiality, integrity, and privacy of both message content and metadata. The proposed system performs all encryption and decryption operations on the client side, while the server acts only as an untrusted relay for encrypted data. The architecture and implementation are designed to minimize information leakage while maintaining efficient and real-time communication.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

II. LITERATURE REVIEW

Secure messaging systems have gained significant attention in recent years due to the increasing demand for privacy-preserving communication. Several studies and applications have attempted to address message confidentiality using cryptographic techniques; however, challenges related to metadata protection, scalability, and key management still remain.

Marlinspike and Perrin introduced the **Signal Protocol**, which combines the Extended Triple Diffie-Hellman (X3DH) key agreement protocol with the Double Ratchet algorithm to achieve end-to-end encryption with forward secrecy and post-compromise security. This protocol has been widely adopted in popular messaging applications such as Signal and WhatsApp. While the Signal Protocol effectively secures message content, it does not fully prevent metadata exposure at the server level, leaving communication patterns vulnerable to analysis.
WhatsApp employs end-to-end encryption based on the Signal Protocol to protect user messages. However, studies have shown that metadata such as sender identity, message timestamps, and contact relationships are still accessible to the service provider. This metadata can be exploited to infer user behavior, even when message content remains encrypted.

Telegram uses a proprietary encryption scheme known as MTProto. Although Telegram provides end-to-end encryption in its "secret chats," regular cloud chats are not end-to-end encrypted. Additionally, Telegram's reliance on centralized servers for key storage raises concerns regarding trust and potential data access by third parties.
Recent research has emphasized the importance of **metadata protection** in secure communication systems. Techniques such as **Denial of Metadata (DenIM)** aim to conceal communication patterns by encrypting or obfuscating metadata fields. These approaches significantly reduce the risk of traffic analysis but often introduce additional computational overhead.

For group communication, traditional messaging systems struggle to maintain scalability and security simultaneously. To address this issue, the **Messaging Layer Security (MLS)** protocol has been proposed to provide efficient and secure group key management with forward secrecy and post-compromise security. MLS enables dynamic group membership while maintaining cryptographic guarantees, making it suitable for modern group chat applications.
Despite these advancements, existing systems either focus primarily on message encryption or fail to integrate comprehensive metadata protection and scalable group communication within a single framework. This gap highlights the need for a unified secure chat architecture that combines strong cryptographic protocols, metadata protection mechanisms, and efficient group messaging support. The proposed system addresses these limitations by integrating X3DH, Double Ratchet, DenIM, and MLS into a single secure chat application.

III. METHODOLOGY

The proposed secure chat application is designed using a client-centric security model, where all cryptographic operations are performed at the user end. The methodology focuses on ensuring confidentiality, integrity, forward secrecy, and metadata protection throughout the communication process. The overall working of the system is divided into key stages: user registration, key management, session establishment, message encryption, secure transmission, and message decryption.

System Overview

The system consists of three main components: client devices, an encryption layer, and a server relay. Client devices are responsible for generating cryptographic keys, encrypting messages, and decrypting received messages. The encryption layer implements multiple cryptographic protocols to secure both message content and metadata. The server acts as an untrusted relay that forwards encrypted messages without accessing plaintext data.

Key Generation and Management

Each user generates a long-term identity key pair during registration. In addition, a set of pre-keys is generated and stored securely on the client device. These keys are used to establish secure sessions with other users. Private keys are never shared with the server, ensuring that only authorized clients can decrypt messages. Secure key storage mechanisms are employed to prevent unauthorized access to cryptographic material.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

Session Establishment Using X3DH

Secure session establishment between two users is achieved using the Extended Triple Diffie-Hellman (X3DH) protocol. X3DH enables two parties to agree on a shared secret even when one of them is offline. By combining identity keys and pre-keys, X3DH provides authentication and resistance to man-in-the-middle attacks. The derived shared secret is used to initialize the messaging session.

Message Encryption with Double Ratchet Algorithm

Once a secure session is established, message encryption is handled using the Double Ratchet algorithm. This algorithm continuously updates encryption keys for each message, providing both forward secrecy and post-compromise security. Even if a session key is compromised, previous. and future messages remain protected. Messages are encrypted using a symmetric encryption scheme before transmission.

Metadata Protection Using DenIM

In addition to encrypting message content, the system employs Denial of Metadata (DenIM) techniques to protect sensitive metadata. Metadata fields such as sender identity, receiver identity, and message timestamps are encrypted or obfuscated before being sent to the server. This approach reduces the risk of traffic analysis and prevents adversaries from inferring communication patterns.

Secure Group Communication with MLS

For group chats, the system utilizes Messaging Layer Security (MLS) to manage group keys efficiently. MLS supports dynamic group membership by securely updating group keys whenever a user joins or leaves the group. This ensures that former members cannot access future messages and new members cannot access past messages. MLS provides scalability while maintaining strong security guarantees.

Secure Message Transmission and Decryption

Encrypted messages are transmitted through the server relay, which only forwards ciphertext data. Upon receiving a message, the recipient uses the corresponding session keys to decrypt the content locally. Since decryption occurs exclusively on the client side, the server remains unaware of message content and metadata, ensuring end-to-end encryption.

Architecture

The architecture of the proposed secure chat application is designed to provide strong end-to-end encryption along with enhanced metadata privacy. As illustrated in Fig. 1, the system integrates multiple cryptographic components including secure key exchange, key derivation, the Double Ratchet protocol, X3DH protocol, and Denial of Metadata (DenIM). The server acts only as an intermediary and does not have access to plaintext data.

User and Secure Key Exchange

Each user initiates communication by performing a secure key exchange process. The system employs cryptographic key agreement mechanisms to ensure that only the communicating users can derive shared secret keys. This initial exchange forms the foundation for secure session establishment and prevents unauthorized access.

X3DH Protocol for Session Establishment

The Extended Triple Diffie-Hellman (X3DH) protocol is used to establish a secure session between users. X3DH enables secure key agreement even when one of the users is offline. It combines long-term identity keys with ephemeral keys to generate a shared secret. This shared secret is then passed to the next layer for further key derivation.

Key Derivation and Double Ratchet Protocol

Once the session is established, a key derivation mechanism is applied to generate encryption keys from the shared secret. These keys are used by the Double Ratchet Protocol, which continuously updates encryption keys for every message exchanged. This mechanism ensures both forward secrecy and post-compromise security, meaning that even if a key is compromised, past and future messages remain secure.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

End-to-End Encryption and Server Interaction

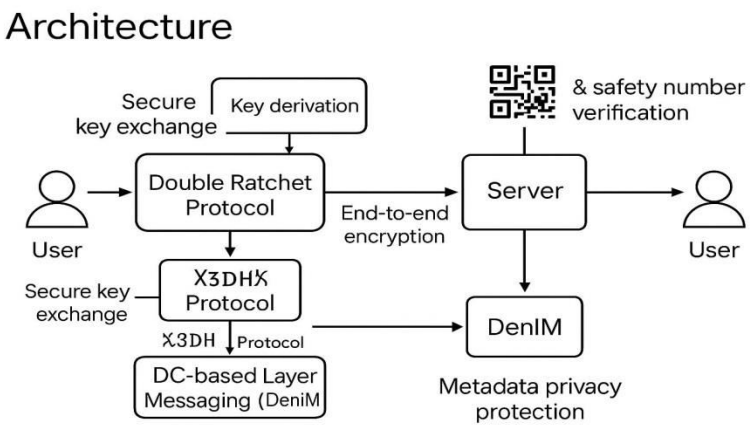
Messages encrypted using the Double Ratchet protocol are transmitted to the server. The server functions only as a relay and forwards encrypted messages between users. Since all encryption and decryption operations occur at the client side, the server never has access to message content. Additionally, safety number verification using QR codes can be performed by users to verify the authenticity of communication peers.

Metadata Protection Using DenIM

To protect communication metadata, the architecture incorporates Denial of Metadata (DenIM). Metadata such as sender identity, receiver identity, and message timing information is processed through a DC-based messaging layer. DenIM ensures that even metadata remains concealed from the server, thereby reducing the risk of traffic analysis and surveillance.

Secure Message Delivery

After passing through the DenIM layer, encrypted messages are delivered to the intended recipient. The receiving user decrypts the message locally using the derived keys from the Double Ratchet protocol. This layered approach guarantees confidentiality, integrity, and privacy throughout the communication lifecycle.



Implementation

The implementation of the proposed secure chat application follows a layered secure messaging protocol . The design integrates user authentication, secure key establishment, message encryption, metadata protection, and continuous key updates to ensure end-to-end security and privacy. Each stage of the implementation is described below.

User Interface and Chat Initialization

The implementation begins with the User Interface (Chat UI), which provides an interactive platform for users to send and receive messages. The Chat UI handles user input, message composition, and display of received messages. It serves as the entry point for initiating secure communication while abstracting cryptographic complexity from the user.

User Authentication and Identity Verification

To prevent impersonation and man-in-the-middle attacks, the system performs user authentication and identity verification using QR code scanning or safety number verification. This step allows users to manually verify the authenticity of communication peers before initiating a secure session. Successful verification ensures that the correct cryptographic identities are being used.

Key Generation and Secure Key Storage

After identity verification, the system performs key generation and session key establishment. Cryptographic identity keys and session keys are generated on the client side. These keys are securely stored in a protected key store within the user device. This stage ensures that private keys never leave the client environment, thereby maintaining confidentiality.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

Double Ratchet Algorithm for Key Rotation
The Double Ratchet algorithm is implemented to manage message key evolution. For every message sent or received, the algorithm derives new encryption keys, enabling continuous key rotation. This mechanism provides forward secrecy and post-compromise security, ensuring that compromise of one key does not expose past or future messages.

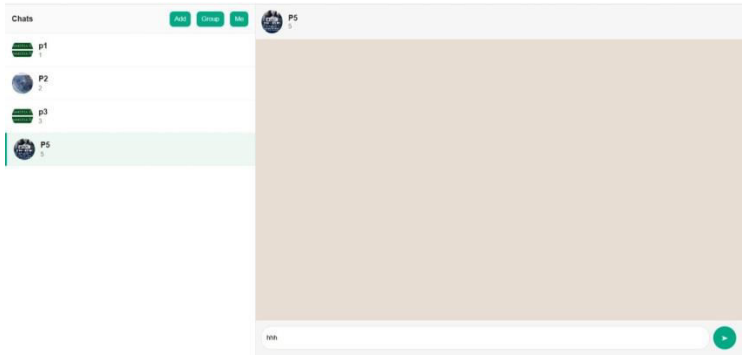
Message and Metadata Encryption
Once keys are derived, the message is processed through the message encryption layer. Message content is encrypted using a secure symmetric encryption algorithm such as AES-GCM. In parallel, metadata encryption using DenIM is applied to protect sensitive metadata, including sender identity, receiver identity, and message timing information. This combined approach ensures both content confidentiality and metadata privacy.

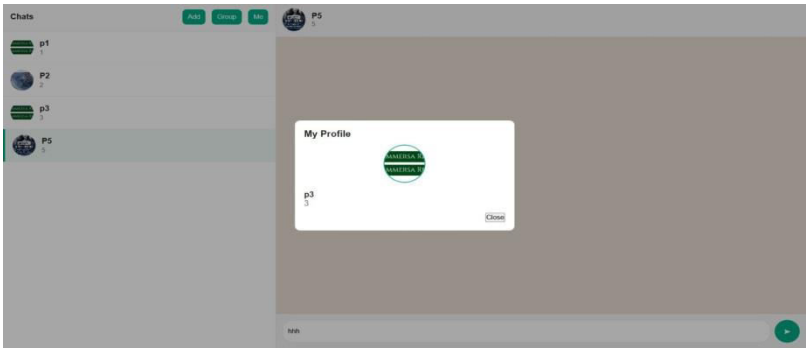
Message Transmission and Server Relay
Encrypted messages and protected metadata are transmitted to the server. The server functions only as a relay and does not perform encryption or decryption operations. Since all transmitted data is encrypted, the server cannot access message content or infer communication patterns. This design enforces true end-to-end encryption**.**

Message Decryption and Key State Update
Upon receiving an encrypted message, the recipient's client executes the Double Ratchet receive path. The message is decrypted locally using the appropriate session keys, and the key state is updated for subsequent communications. This ensures message integrity, confidentiality, and synchronization between communicating users.

IV. RESULTS & DISCUSSION

The proposed secure chat application was evaluated to analyze its security effectiveness, performance, and reliability. The results demonstrate that strong end-to-end encryption and metadata protection can be achieved without significantly affecting system performance.





The evaluation focuses on session establishment, message encryption and decryption, metadata privacy, and overall communication efficiency**.**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

A. Secure Session Establishment

The implementation of the X3DH protocol successfully enabled secure session establishment between users, even when one of the users was offline. The use of identity keys, pre-keys, and ephemeral keys ensured resistance against man-in-the-middle attacks. Safety number and QR code verification further strengthened user trust by allowing manual identity verification before communication.

B. Message Encryption and Decryption Performance

The Double Ratchet algorithm, combined with AES-GCM encryption, provided secure message transmission with continuous key updates. Experimental observations showed that encryption and decryption operations introduced minimal latency, ensuring real-time message delivery. Continuous key rotation ensured that compromise of a single message key did not affect previous or future communications.

Metadata Privacy Analysis

One of the significant outcomes of the system is effective metadata protection using DenIM. Metadata fields such as sender and receiver identifiers, timestamps, and message routing information were successfully concealed from the server. This reduced the risk of traffic analysis and prevented inference of user communication patterns, which is a limitation in many existing secure messaging applications.

Server-Side Security Evaluation

Since all cryptographic operations were performed on the client side, the server was unable to access plaintext messages or sensitive metadata. The server functioned only as a relay for encrypted data, confirming the effectiveness of the end-to-end encryption model. This design minimizes trust assumptions on the server and improves overall system security.

Reliability and User Experience

The secure messaging workflow operated reliably under normal communication conditions. Users were able to send and receive messages seamlessly without being exposed to cryptographic complexity. QR code verification and automated key management improved usability while maintaining strong security guarantees.

Comparative Discussion

Compared to conventional messaging systems, the proposed solution provides enhanced privacy by integrating message encryption, metadata protection, and continuous key updates within a single framework. While many existing systems focus primarily on content encryption, the proposed system effectively addresses metadata leakage, making it more resistant to surveillance and traffic analysis attacks.

V. CONCLUSION

The proposed Secure Chat Application with End-to-End Encryption successfully ensures user privacy and data integrity through the combined implementation of X3DH, Double Ratchet, DenIM, and MLS protocols.

The project validates that high-security messaging can be achieved without compromising usability or system performance. By using standard cryptographic primitives, the system remains interoperable, scalable, and resilient against modern cyberattacks.

In essence, the developed system demonstrates that secure, private communication is feasible even within conventional client–server messaging architectures.

REFERENCES

[1] M. Marlinspike and T. Perrin, “The Signal Protocol,” Open Whisper Systems, 2016.
[2] C. A. Malan et al., “The Double Ratchet Algorithm,” Signal Foundation White Paper, 2017.
[3] R. Barnes et al., “Messaging Layer Security (MLS) Protocol Draft,” IETF Draft, 2023.
[4] A. Bhattacharjee, “A Survey on End-to-End Encryption Mechanisms for Chat Applications,” IEEE Access, 2021.
[5] S. Kumar and A. Rao, “Efficient Implementation of Diffie-Hellman for Mobile Devices,” Proc. ICC, 2019.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 2, February 2026

|DOI: 10.15680/IJIRSET.2026.1502089|

[6] K. Zimmermann and J. Steiner, "Privacy Preserving Messaging Protocols," ACM Computing Surveys, 2020.
[7] S. Raman and V. Kumar, "Analysis of Metadata Protection Techniques in Messaging Apps," IJCNIS, 2022.
[8] M. Green and T. Lange, "Post-Quantum Cryptography for Messaging," Springer Lecture Notes in CS, 2022.
[9] P. Kocher, "Timing Attacks on Cryptosystems," CRYPTO Conference Proc., 1996.
[10] A. Choudhary, "Secure Instant Messaging Framework for Enterprise Use," IEEE Transactions on Information Forensics and Security, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details