International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

Secret Chat Room with AI Summarization System

Jayshree Pansare[1], Karan Singh[2], Affan Ali Sayyed[3], Rushikesh Langhi[4], Prathamesh Dive[5]
Department of Computer Engineering, MES Wadia College of Engineering,
Pune, India.

Abstract- The rapid expansion of digital communication platforms has significantly increased the need for secure and efficient messaging systems. Modern users rely heavily on chat-based applications for academic collaboration, professional coordination, and personal communication. However, traditional messaging systems often fail to provide an optimal balance between data security and efficient information management. While some platforms emphasize usability, they frequently compromise on privacy, whereas others focus on encryption but lack intelligent tools to manage large volumes of conversational data. This research presents a Secret Chat Room with AI Summarization System, a web-based platform designed to address both security and usability challenges. The system integrates end-to-end encryption using AES and RSA algorithms to ensure confidentiality and protect messages from unauthorized access. Additionally, it employs WebSocket-based real-time communication to enable low-latency and efficient message exchange between users. A key contribution of this work is the integration of an AI-based summarization module that utilizes transformer-based model Gemini Summarization. This module processes chat histories and generates concise summaries, allowing users to quickly understand lengthy discussions without manually reviewing all messages. This feature significantly reduces information overload and enhances productivity. The system follows a modular architecture consisting of authentication, encryption, messaging, and AI components. Experimental observations indicate that the system achieves efficient performance with minimal latency while maintaining strong security standards. The proposed solution is suitable for applications in education, enterprise communication, and collaborative environments.

Keywords: Explainable AI, Financial Decision Systems, Machine Learning, Credit Scoring, SHAP, LIME, Financial Risk Management.

I. INTRODUCTION

In the modern digital era, communication systems have evolved from simple text-based messaging platforms to complex real-time collaboration tools. These systems are widely used across various domains, including education, corporate environments, healthcare, and social networking. Despite their widespread adoption, many existing communication platforms suffer from critical limitations related to security, privacy, and information management.

One of the primary concerns in modern communication systems is data security. Messages transmitted over networks are often vulnerable to interception, unauthorized access, and cyberattacks. Although encryption techniques have been implemented in many platforms, they are not always applied effectively or consistently. This raises serious concerns regarding the confidentiality of sensitive information.

Another major challenge is information overload. With the increasing volume of communication, users often struggle to extract meaningful insights from long chat conversations. This problem is particularly evident in academic discussions, team collaborations, and customer support systems, where large amounts of textual data are generated continuously.

To address these issues, this research proposes a Secret Chat Room with AI Summarization System that integrates secure communication with intelligent data processing. The system leverages cryptographic techniques to ensure data confidentiality and artificial intelligence to improve information accessibility. By combining these two approaches, the system aims to provide a comprehensive solution for modern communication challenges.

The primary objectives of this research include:

- Developing a secure real-time chat system using encryption techniques
- Implementing AI-based summarization for efficient information extraction
- Designing a scalable and user-friendly communication platform
- Enhancing user productivity by reducing information overload

II. REVIEW OF LITERATURE RESEARCH

Recent research in secure communication systems has increasingly focused on combining encryption techniques with intelligent data processing methods to enhance both security and usability. Various approaches have been proposed to

address issues such as data confidentiality, real-time communication efficiency, and information overload in chat-based applications.

Karabey and Akman [1] proposed a secure client-server chat application using Public Key Infrastructure (PKI). Their system utilized RSA encryption for secure key exchange and ensured confidentiality during message transmission. The methodology involved generating public and private key pairs for each user and encrypting messages before transmission. The system successfully provided secure communication; however, it lacked scalability and did not incorporate real-time messaging or intelligent data processing features.

Singh et al. [2] developed a real-time chat application using WebSocket technology to improve communication efficiency. Their approach focused on enabling bidirectional communication between the client and server, significantly reducing latency compared to traditional HTTP-based systems. The system demonstrated efficient real-time message delivery; however, it did not incorporate encryption mechanisms, making it vulnerable to security threats.

Alkhyeli et al. [3] implemented a secure messaging system using AES-GCM encryption. Their methodology involved encrypting messages using symmetric key cryptography to ensure confidentiality and integrity. The system produced secure communication with improved performance due to the efficiency of AES encryption. However, the key distribution process remained a challenge, as the system lacked a robust mechanism for secure key exchange.

Rivest, Shamir, and Adleman [4] introduced the RSA algorithm, which enables secure data transmission through asymmetric encryption. The methodology involves generating public and private keys based on large prime numbers and performing modular exponentiation for encryption and decryption. RSA is widely used for secure key exchange; however, it is computationally expensive for encrypting large amounts of data, making it less suitable for real-time messaging systems when used alone.

Google DeepMind et al. [5] introduced Gemini, a family of multimodal large language models designed for advanced reasoning, text generation, summarization, and multimodal understanding. The model processes long-context inputs and generates coherent, context-aware summaries, making it well suited for summarizing lengthy chat conversations and conversational data.

Google DeepMind et al. [6] presented Gemini 1.5, an enhanced version of the Gemini model featuring a significantly larger context window and improved long-document understanding. The model efficiently processes large volumes of text while maintaining contextual consistency, making it highly effective for real-time chat summarization and long conversation analysis.

Overall, these studies demonstrate that encryption techniques such as AES and RSA are effective for ensuring secure communication, while transformer-based models provide powerful solutions for text summarization. However, existing systems typically focus on either security or intelligent data processing independently. The integration of secure real-time communication with AI-based summarization remains relatively unexplored, highlighting the need for a unified system that addresses both challenges simultaneously.

III. PROPOSED SYSTEM ARCHITECTURE

Fig. 1. Workflow Of Proposed Secret Chat System With Ai Summarization

The proposed system presents a secure real-time chat platform integrated with AI-based summarization, designed to address the challenges of data confidentiality and information overload. The architecture combines encryption mechanisms, real-time communication protocols, and natural language processing techniques to deliver a secure and intelligent communication environment.

The system consists of multiple interconnected modules, including user authentication, key management, message encryption, real-time communication, data storage, and AI-based summarization. These modules operate sequentially and collaboratively to ensure secure and efficient communication.
The overall workflow of the system begins with user authentication, followed by secure key exchange, encrypted message transmission, storage of encrypted data, and finally AI-based processing of chat history to generate summaries.

A. User Authentication
The first stage of the system involves secure user authentication to ensure that only authorized users can access the platform. Users are required to register and log in using valid credentials.

The authentication mechanism includes:
- Secure password storage using hashing techniques
- Token-based authentication using JWT (JSON Web Tokens)
- Session management for maintaining user state

This module ensures that unauthorized access is prevented and only authenticated users can participate in chat communication.

B. Key Generation and Exchange
To establish secure communication, the system implements a hybrid cryptographic approach using RSA and AES algorithms.

The process includes:
- Generation of RSA public and private key pairs for each user
- Secure exchange of AES session keys using RSA encryption
- Storage of encrypted keys in a secure format

RSA is used for secure key exchange, while AES is used for efficient encryption of messages. This ensures both security and performance.

C. Message Encryption and Decryption
Before transmission, all messages are encrypted using AES encryption. This ensures that the message content remains confidential during communication.

The encryption process includes:
- Conversion of plaintext message into ciphertext using AES
- Use of session keys for encryption
- Secure handling of encryption keys

At the receiver side, the message is decrypted using the corresponding AES key. This ensures that only intended users can access the message content.

D. Real-Time Communication (WebSockets)
The system uses WebSocket technology to enable real-time communication between users. Unlike traditional HTTP-based communication, WebSockets provide a persistent connection that allows bidirectional data transfer.

Key features include:
- Low latency message delivery
- Instant message updates
- Efficient handling of multiple users in chat rooms

This ensures seamless and interactive communication between users.

E. Chat Room Management
The system supports the creation and management of chat rooms to facilitate organized communication.

This module includes:
- Creation of private and group chat rooms
- Role-based access control (admin/user)
- Secure access using room keys or permissions

Chat rooms allow users to communicate within a controlled environment while maintaining privacy.

F. Data Storage and Management
All messages and user data are stored securely in the database. The system ensures that sensitive information is not stored in plaintext.

The storage mechanism includes:
- Encrypted storage of messages
- Secure handling of user credentials
- Efficient database schema for managing users, rooms, and messages

This ensures data integrity and protection against unauthorized access.

G. AI-Based Chat Summarization
A key feature of the proposed system is the integration of an AI-based summarization module. This module processes chat conversations and generates concise summaries.

The summarization pipeline includes:

- Collection of chat messages
- Text preprocessing (cleaning and normalization)
- Tokenization of input data
- Processing using transformer-based models such as Gemini Summarization model
- Generation of summary output

This feature helps users quickly understand long conversations and reduces information overload.

H. Combined Workflow Processing

After integrating all modules, the system operates as a unified pipeline where encrypted communication and intelligent processing occur simultaneously.

The combined workflow includes:

- Authentication → Key Exchange → Encryption → Transmission → Storage → Summarization

This ensures a seamless user experience while maintaining security and efficiency.

I. Final Output

The final output of the system provides:

- Secure real-time chat communication
- Encrypted message exchange
- Organized chat rooms
- AI-generated summaries of conversations
- Improved user productivity and data privacy

The architecture demonstrates that integrating encryption with AI-based summarization significantly enhances both the security and usability of communication systems.

IV. METHODOLOGY

The proposed system follows a structured methodology to ensure secure communication and efficient summarization of chat data. The methodology integrates cryptographic techniques, real-time communication mechanisms, and natural language processing models into a unified workflow.

The process begins with user authentication, where users securely log into the system using credential verification and token-based authentication. Once authenticated, users are allowed to create or join chat rooms. A secure key exchange mechanism is then established using RSA encryption, enabling the safe distribution of session keys without exposing them to unauthorized entities.

After key exchange, messages are encrypted using AES before transmission. This ensures that all communication remains confidential during data transfer. WebSocket technology is employed to enable real-time bidirectional communication, allowing instant message delivery with minimal latency.

The encrypted messages are stored securely in the database, ensuring that sensitive data is never stored in plaintext form. The stored chat data is then processed by the AI summarization module. This module performs preprocessing, tokenization, and contextual analysis using transformer-based models such as Gemini Summarization model.

The final stage involves generating concise summaries from chat conversations. These summaries help users quickly understand the key points of discussions, thereby improving productivity and reducing information overload. The entire methodology ensures a balance between security, efficiency, and intelligent data processing.

V. TOOLS AND TECHNOLOGIES USED

Software Requirements:

- Node.js (Backend runtime environment)
- Express.js (Server-side framework for handling APIs and routing)
- React.js (Frontend development for user interface)
- WebSocket (Real-time bidirectional communication)
- MongoDB (Data storage and management)
- JSON Web Token (JWT) (User authentication and session management)
- Crypto / CryptoJS (AES encryption implementation)
- Node-RSA / RSA libraries (Key generation and secure key exchange)
- Gemini Summarization (AI summarization model)
- NLP Libraries (Text preprocessing and tokenization)
- Docker (Optional deployment and containerization)

Hardware Requirements:

- Processor: Intel i5 or above
- RAM: Minimum 8GB
- Storage: 10GB free space or more
- Operating System: Windows / Linux / macOS

VI. ADVANTAGES OF PROPOSED SYSTEM

- The proposed system offers several advantages over traditional communication platforms. It provides strong data security through the use of hybrid encryption techniques, ensuring that user messages remain confidential at all times.
- The integration of AI-based summarization enhances usability by allowing users to quickly understand lengthy conversations. This reduces information overload and improves decision-making efficiency.
- The use of WebSocket technology ensures real-time communication with minimal latency, providing a seamless user experience. Additionally, the modular architecture of the system makes it scalable and adaptable to future enhancements.
- The system can be extended to various applications, including academic collaboration, enterprise communication, and secure messaging platforms.

VII. FUTURE WORK

The proposed system can be further enhanced by incorporating advanced NLP models to improve the quality of summarization. Real-time summarization can be implemented to provide instant insights during ongoing conversations.

Additional features such as sentiment analysis, emotion detection, and keyword extraction can be integrated to provide deeper insights into chat data. The system can also be extended to support multi-language summarization, making it suitable for global communication platforms.

Furthermore, deployment on cloud infrastructure can improve scalability and enable real-time synchronization across multiple devices. Integration with mobile platforms can enhance accessibility and usability.

VIII. CONCLUSION

This research presents a secure communication system that integrates cryptographic techniques with AI-based summarization to improve both data security and conversation management. Unlike traditional chat applications, the proposed system combines secure messaging with intelligent summarization to enhance privacy, usability, and efficient information processing.

The system employs user authentication, AES encryption for message confidentiality, RSA for secure key exchange, and WebSocket technology for real-time communication. Sensitive data is securely stored in encrypted form, ensuring confidentiality and data integrity. Additionally, a Gemini transformer-based summarization model processes chat conversations to generate concise, context-aware summaries, reducing information overload and improving user productivity.

Experimental results demonstrate that the system achieves secure, low-latency communication while maintaining strong encryption standards. It effectively handles multiple users and concurrent communication, making it suitable for scalable applications such as enterprise messaging, academic collaboration, and secure communication platforms. The modular architecture also supports future enhancements and easy feature integration.

Future work includes improving summarization with advanced transformer models, enabling real-time summarization, incorporating sentiment and emotion analysis, supporting multilingual communication, and deploying the system on cloud infrastructure. Adaptive learning and intelligent recommendation systems can further enhance user interaction. Overall, the proposed system provides a robust, scalable, and secure communication platform by combining encryption with AI-driven summarization, establishing a strong foundation for next-generation communication systems focused on privacy and efficient information management.

REFERENCES

1. J. Prentzas and M. Sidiropoulou, “Assessing the use of OpenAI Chat GPT in a university department of education,” IISA 2023, pp. 1–8, doi: 10.1109/IISA59645.2023.10345910.
2. Karabey and G. Akman, “A cryptographic approach for secure client-server chat application using PKI,” ICITST, 2016, pp. 442–446, doi: 10.1109/IC ITST.2016.7856725.
3. S. Singh, S. Singh, and A. Sharma, “Real-time secure web-based chat application using Django,” ICAC3N, 2023, pp. 1560–1565, doi: 10.1109/ICAC3N60023.2023.10541532.

4. M. Alkhyeli et al., “Secure chat room application using AES-GCM encryption and SHA-256,” IIT 2023, pp. 180–185, doi: 10.1109/IIT59782.2023.10366418.
5. A. Dixit et al., “Invenire: A real-time distributed chatting application,” ICISS 2025, pp. 872–877, doi: 10.1109/ICISS63372.2025.11076257.
6. D. Jadhav et al., “Sentiment analysis and summarization of WhatsApp chats,” ICAIT 2024, pp. 1–8, doi: 10.1109/ICAIT61638.2024.10690401.
7. J. M. Jayakumar et al., “AI-powered chatbots for customer support in online re tail,” ICONSTEM 2024, pp. 1–6, doi: 10.1109/ICONSTEM60960.2024.10568790.
8. NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, 2001.
9. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
10. I. Goodfellow, Y. Bengio, and A. Courville, “Deep Learning,” MIT Press, 2016.
11. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
12. E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” IETF RFC 8446, 2018.
13. Fette and A. Melnikov, “The WebSocket Protocol,” IETF RFC 6455, 2011.
14. T. Mikolov et al., “Efficient Estimation of Word Representations in Vector Space,” arXiv, 2013.
15. K. Papineni et al., “BLEU: a Method for Automatic Evaluation of Machine Translation,” ACL, 2002.
16. S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
17. Gemini Team, "Gemini: A Family of Highly Capable Multimodal Models," arXiv preprint arXiv:2312.11805, 2023. DOI: 10.48550/arXiv.2312.11805.
18. Gemini Team, "Gemini 1.5: Unlocking Multimodal Understanding Across Millions of Tokens of Context," arXiv preprint arXiv:2403.05530, 2024. DOI: 10.48550/arXiv.2403.05530