Intelligent Systems Research and Applications Journal

www.israj.org
eISSN:3120-0826

Block-Crypt Chat: Secure Messaging Reinvented with Blockchain and Real - Time Encryption

Alpa Patel[1,*], Sindhu S[2], Rakshitha S[3]

[1] School of Computer Applications, Dayananda Sagar University, Bengaluru, Karnataka, India
[2] School of Computer Applications, Dayananda Sagar University, Bengaluru, Karnataka, India
[3] School of Computer Applications, Dayananda Sagar University, Bengaluru, Karnataka, India

ARTICLE INFO

Article history:
Received 2 April 2026
Received in revised form 25 May 2026
Accepted 2 June 2026
Available online 7 June 2026

Keywords:
Blockchain; Cryptography; End-to-End Encryption; Real-Time Communication; Secure Messaging; SHA-256

ABSTRACT

The increasing demand for secure and trustworthy digital communication necessitates advanced solutions beyond traditional centralized messaging systems. This paper proposes a blockchain-enabled secure messaging framework that integrates hybrid RSA-AES encryption with real-time communication mechanisms. The system ensures end-to-end confidentiality by performing client-side encryption, while message integrity is maintained through SHA-256 hash logging on a blockchain, enabling tamper-proof verification without revealing message content. Additionally, a PIN-based secure file-sharing mechanism enhances data protection. The proposed model is implemented using a modern web-based architecture and evaluated for performance and security. Experimental results indicate low latency, strong data protection, and improved transparency compared to existing systems. The framework demonstrates scalability and practical applicability in sensitive domains such as enterprise communication, education, and legal environments.

1. Introduction

In the digital era, secure communication has become a critical requirement due to the rapid growth of online interactions across personal, corporate, and governmental domains. Traditional messaging platforms, although widely used, often rely on centralized architectures that introduce vulnerabilities such as data breaches, unauthorized access, and lack of transparency. While modern applications incorporate end-to-end encryption (E2EE), they still depend on centralized servers for key management and message routing, which raises concerns regarding trust and data integrity [20], [5]. Consequently, there is a growing need for decentralized, verifiable, and tamper-proof communication systems that can ensure both privacy and accountability.

Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized and immutable ledger for storing transaction records. Its inherent properties, such as transparency, security, and resistance to tampering, make it suitable for secure communication systems [13], [23]. Several studies have explored the integration of blockchain with

*Corresponding author.
E-mail address: alpa8187@gmail.com
https://doi.org/10.59543/j02krs95

messaging platforms to enhance trust and auditability. For instance, decentralized messaging architectures have been proposed to eliminate single points of failure and reduce reliance on third-party intermediaries [1], [8]. Additionally, blockchain-based systems have demonstrated effectiveness in ensuring message authenticity and integrity through cryptographic hashing and smart contracts [18], [22].

Alongside blockchain, cryptographic techniques play a vital role in securing communication. Hybrid encryption models combining asymmetric algorithms such as RSA and symmetric algorithms such as AES offer both security and efficiency [6], [19]. RSA is commonly used for secure key exchange, while AES provides fast encryption of message content. Such hybrid approaches have been widely adopted in secure messaging systems to achieve confidentiality, integrity, and authentication [21], [9]. Furthermore, advancements in secure file sharing and identity verification mechanisms have strengthened the reliability of communication systems in sensitive domains such as healthcare, legal, and academic environments [10], [16].

Despite these advancements, existing systems still face several limitations, including lack of real-time performance, absence of user-friendly interfaces, inadequate file protection mechanisms, and limited support for independent message verification. Many solutions either focus heavily on backend security or fail to provide scalable and practical implementations suitable for real-world usage [7], [15]. Moreover, issues such as blockchain scalability and efficient integration with real-time communication frameworks remain open research challenges [25], [4]. Therefore, there is a need for a comprehensive system that integrates blockchain, encryption, and real-time communication technologies into a unified, scalable, and user-centric platform.

To address these challenges, this paper proposes a secure messaging system that combines blockchain-based logging with hybrid RSA-AES encryption and real-time communication using modern web technologies. The system ensures end-to-end encryption, tamper-proof message verification, and secure file sharing with additional protection mechanisms. By leveraging blockchain for storing message hashes, the proposed approach enhances trust and provides an auditable communication trail without compromising user privacy [3], [12].
The primary objectives of this research are as follows:

- To design and develop a secure real-time chat system using hybrid RSA and AES encryption.
- To integrate blockchain technology for tamper-proof logging of message and file hashes.
- To ensure end-to-end privacy and confidentiality in communication.
- To implement secure file sharing with additional protection mechanisms such as PIN-based access.
- To enhance system usability with real-time features such as instant messaging and delivery status.
- To provide a scalable and modular architecture for future extensions such as group communication and decentralized identity.

Recent advancements in secure communication systems have increasingly focused on integrating cryptographic techniques with decentralized technologies to enhance privacy, integrity, and trust. Blockchain-based messaging frameworks have gained significant attention due to their

ability to provide tamper-proof and transparent communication records. For instance, Ahmed et al. [1] proposed a decentralized messaging architecture that leverages blockchain to eliminate reliance on centralized servers, thereby reducing vulnerabilities associated with single points of failure. Similarly, Singh et al. [20] developed an end-to-end encrypted messaging system where public keys are stored on a blockchain, ensuring authenticity and preventing key tampering.

Several studies have explored hybrid encryption mechanisms to improve both security and performance. Das et al. [6] introduced a secure chat system combining RSA and AES encryption, where RSA is used for secure key exchange and AES for efficient data encryption. Sharma and Singh [19] further emphasized that hybrid encryption models offer a balance between computational efficiency and robust security. These approaches are particularly suitable for real-time applications where latency and security must be optimized simultaneously. Additionally, Tanveer et al. [21] demonstrated the application of AES-based secure communication in institutional environments, highlighting improved confidentiality and controlled access.

Blockchain integration has also been widely investigated for ensuring message integrity and auditability. Rajput et al. [18] utilized smart contracts to store message hashes, enabling tamper-proof communication logs for enterprise applications. Wang and Hu [22] extended this concept by proposing blockchain-based messaging systems that provide legally admissible communication records, particularly useful in legal and compliance-driven environments. Furthermore, Pandey et al. [16] developed a blockchain-enabled academic communication system that ensures transparency and accountability between students and faculty.

Decentralized storage and communication frameworks have also been explored to enhance system resilience. Lin et al. [14] proposed a decentralized chat system using blockchain and IPFS, enabling secure and distributed data storage. Similarly, Hassan et al. [8] designed a peer-to-peer messaging system that eliminates centralized control and improves resistance to cyberattacks. These approaches highlight the potential of decentralized architectures in building secure and scalable communication platforms. However, scalability remains a concern, as discussed by Zhou et al. [25], who identified performance bottlenecks in blockchain-based systems due to transaction overhead and network latency.

In addition to communication security, identity verification and access control have been addressed in several works. Kumar and Sharma [12] proposed a decentralized identity management system integrated with blockchain to prevent impersonation and unauthorized access. Zhao and Li [24] focused on secure file sharing with blockchain-based hash verification, ensuring data integrity during transmission. Similarly, Islam et al. [9] highlighted the importance of encryption in secure file sharing systems, emphasizing the need for robust access control mechanisms.

Despite these advancements, several research gaps remain. First, many existing systems focus primarily on backend security while neglecting real-time communication features and user-friendly interfaces, limiting their practical adoption [7], [15]. Second, most blockchain-based messaging solutions store only partial data, such as keys or metadata, rather than continuous message verification logs, reducing transparency and auditability [4]. Third, secure file-sharing mechanisms often lack additional protection layers, such as PIN-based or multi-factor authentication, which are essential for sensitive data exchange. Fourth, scalability and performance challenges persist in blockchain integration, particularly in real-time applications [25]. Finally, there is limited work on integrating all key components—hybrid encryption, blockchain logging, real-time communication, and usability—into a single unified framework.

To address these gaps, the proposed system aims to develop a comprehensive secure messaging platform that combines real-time communication, hybrid RSA-AES encryption,

blockchain-based message verification, and enhanced usability features, thereby providing a scalable and practical solution for modern secure communication needs.

Recent research has increasingly focused on enhancing secure communication systems by combining advanced cryptographic techniques with decentralized architectures. For instance, recent studies have explored hybrid encryption frameworks that integrate symmetric and asymmetric algorithms to improve both efficiency and security in communication systems. Furthermore, blockchain-based communication models have been proposed to ensure data integrity, transparency, and resistance to tampering in distributed environments. In 2024, several works emphasized the importance of secure cross-chain communication and interoperability, highlighting challenges in transferring data across heterogeneous blockchain networks. Similarly, blockchain-powered frameworks incorporating attribute-aware encryption have been developed to enhance access control and data confidentiality in cloud-based communication systems. Recent advancements also include lightweight encryption mechanisms designed for resource-constrained environments such as IoT-based healthcare systems, ensuring secure and efficient data exchange. Moreover, modern secure messaging protocols are being designed with strong security guarantees such as forward secrecy, mutual authentication, and resistance to compromise attacks. Emerging research trends are also moving toward post-quantum cryptographic approaches, integrating classical and quantum-resistant algorithms to safeguard future communication systems against quantum threats. Despite these advancements, many existing solutions either lack real-time communication capabilities or fail to integrate all critical components such as encryption, blockchain verification, and usability into a unified framework. Therefore, there remains a need for comprehensive systems that effectively combine security, performance, and practical deployment considerations in modern communication environments.

Finally, the remainder of this paper is organized as follows. Section 2 describes the methodology, including system architecture, encryption techniques and block-chain integration. Section 3 discusses the results and performance evaluation of the proposed system. Section 4 concludes the paper with key findings and outlines future research directions.

2. Methodology

This section presents the design and implementation methodology of the proposed secure messaging system, which integrates hybrid cryptographic techniques, blockchain-based verification, and real-time communication. The methodology is structured to ensure confidentiality, integrity, authenticity, and scalability while maintaining usability for end users. The overall workflow follows a modular architecture consisting of the client layer, server layer, cryptographic layer, and blockchain layer.

2.1 System Architecture Overview

The proposed model adopts a client-server architecture enhanced with decentralized verification. The frontend is developed using a modern web framework to handle user interaction, while the backend manages communication logic, authentication, and data processing. Real-time communication is facilitated through WebSocket-based protocols, enabling low-latency message exchange between users. Unlike conventional systems, the proposed architecture ensures that sensitive cryptographic operations, such as key generation and encryption, are performed on the client side, thereby minimizing server-side exposure.

The system integrates four primary components:

1. User Interface Layer – Handles login, messaging, and file-sharing operations.
2. Communication Layer – Ensures real-time transmission of encrypted messages.
3. Cryptographic Layer – Implements hybrid RSA-AES encryption.
4. Blockchain Layer – Stores message hashes for integrity verification.

Table 1 presents the architectural components of the proposed secure messaging system along with their respective functionalities. The system is divided into four major layers: user interface, communication, cryptographic, and blockchain. Each layer performs a specific role, ensuring modularity, scalability, and security. This layered design helps in efficient integration of real-time communication, encryption mechanisms, and tamper-proof verification using blockchain technology.

Table 1

System Components and Their Functions

Component Layer	Module/Element	Function Description
User Interface Layer	Chat Interface	Enables users to send/receive messages and files in real time
	Authentication Module	Handles login with CAPTCHA verification
Communication Layer	WebSocket Protocol	Provides real-time bidirectional communication
	Message Routing System	Transfers encrypted messages between users
Cryptographic Layer	RSA Algorithm	Used for secure key exchange
	AES Algorithm	Encrypts message content and files
	Key Management Module	Generates and stores public-private keys
Blockchain Layer	SHA-256 Hash Generator	Creates hash of encrypted messages
	Smart Contract	Stores message hashes on blockchain
	Verification Module	Validates message integrity using stored hashes

Figure 1 shows the architecture which integrates a hybrid RSA-AES encryption layer on the client side to ensure end-to-end confidentiality and secure key exchange. It utilizes a WebSocket-based server for low-latency, real-time message routing while simultaneously logging message hashes on a blockchain ledger for tamper-proof integrity verification. This decentralized approach eliminates reliance on a single central authority, ensuring that messages are both private and verifiable.

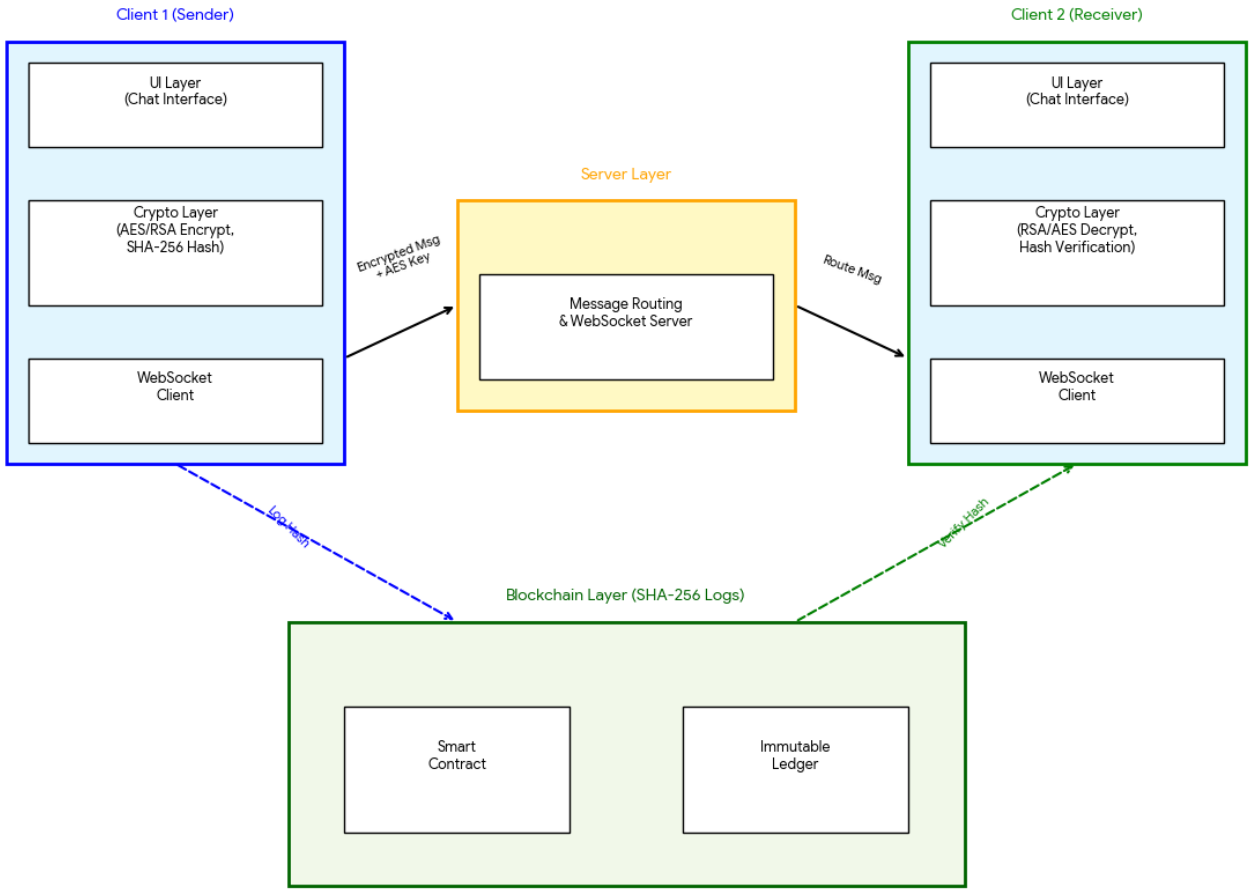

Fig. 1. Proposed System Architecture

2.2 Cryptographic Model

The proposed system employs a hybrid encryption approach combining asymmetric and symmetric cryptography. Initially, each user generates an RSA public-private key pair locally. The public key is shared with other users, while the private key remains securely stored on the client device.

When a user sends a message, the following steps are executed:

- A random AES session key is generated for encrypting the message content.
- The plaintext message is encrypted using AES, ensuring fast and efficient encryption.
- The AES key is then encrypted using the recipient's RSA public key.
- The encrypted message and encrypted AES key are transmitted together.

At the receiver's end, the AES key is decrypted using the private RSA key, followed by decryption of the message content. This hybrid mechanism ensures both security and computational efficiency, making it suitable for real-time communication.

2.3 Blockchain-Based Integrity Verification

To ensure tamper-proof communication, the system incorporates a blockchain-based logging mechanism. Instead of storing actual messages on the blockchain, which would be inefficient and

privacy-invasive, the system computes a SHA-256 hash of each encrypted message. This hash acts as a unique fingerprint of the message.

The hash, along with metadata such as timestamp and sender-receiver identifiers, is recorded on the blockchain using smart contract transactions. This approach provides the following advantages:

- **Immutability:** Once stored, the hash cannot be altered.
- **Auditability:** Users can verify message integrity by recomputing and comparing hashes.
- **Privacy Preservation:** No actual message content is exposed on-chain.

2.4 Secure File Sharing Mechanism

In addition to text messaging, the system supports secure file transfer. Files are encrypted using AES before transmission, ensuring confidentiality. To enhance security, a user-defined PIN is associated with each file. This PIN acts as an additional authentication factor required during file download.

The process includes:

- File encryption using AES.
- Secure upload to the server.
- PIN validation during download.
- Decryption after successful verification.

This dual-layer protection mechanism prevents unauthorized access even if the file is intercepted.

2.5 Real-Time Communication Flow

The system utilizes a WebSocket-based communication protocol to enable real-time interaction. This workflow ensures secure, real-time, and verifiable communication as given below in figure 2.

The message transmission flow is as follows:

1. User authentication is completed with CAPTCHA verification.
2. The sender composes a message and selects the recipient.
3. The message is encrypted using AES, and the AES key is encrypted using RSA.
4. A SHA-256 hash of the encrypted message is generated.
5. The hash is stored on the blockchain via a smart contract.
6. The encrypted message and key are transmitted through the server using WebSockets.
7. The receiver decrypts the AES key and message using their private key.
8. The message is displayed in the user interface.

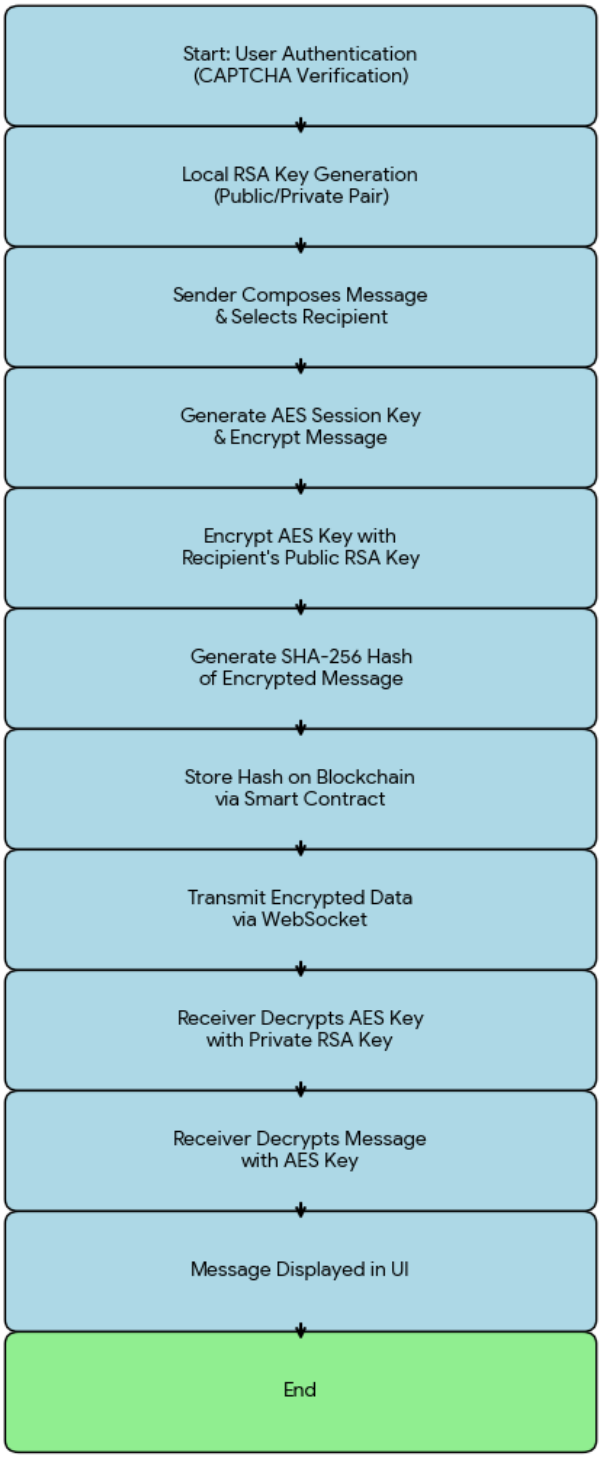

Fig. 2. Proposed Block-Crypt Chat Workflow

2.6 Scalability and Design Considerations

The system is designed with modularity and scalability in mind. Each component operates independently, allowing future integration of advanced features such as group communication, decentralized identity management, and multimedia support. Additionally, blockchain interactions can be optimized using Layer-2 solutions to reduce latency and transaction costs.

Overall, the proposed methodology provides a comprehensive framework that integrates encryption, blockchain, and real-time communication into a unified system. This approach not only enhances security and trust but also ensures practical usability, making it suitable for deployment in real-world secure communication scenarios.

3. Results and Discussion

The proposed secure messaging system was implemented and evaluated to analyze its performance, security, and usability in real-time communication scenarios. The system integrates hybrid encryption (RSA-AES), blockchain-based message verification, and WebSocket-based real-time communication, providing a comprehensive solution for secure and verifiable messaging. The results demonstrate that the system effectively achieves its intended objectives of confidentiality, integrity, and low-latency communication.

3.1 System Performance Evaluation

The system was tested under a controlled environment with multiple users communicating simultaneously. The use of AES encryption for message content ensured minimal computational overhead, while RSA was efficiently utilized for secure key exchange. The hybrid approach resulted in fast encryption and decryption processes, making the system suitable for real-time applications. Message transmission latency remained low due to the implementation of WebSocket-based communication, which eliminates the need for repeated HTTP requests.Blockchain integration was evaluated by logging SHA-256 hashes of messages. It was observed that storing only hash values significantly reduced blockchain overhead compared to storing full message content. The hash generation process was computationally efficient and did not introduce noticeable delays in message delivery. However, transaction confirmation time on the blockchain may vary depending on network conditions, which can impact real-time verification but not message delivery itself.

3.2 Security Analysis

The system provides multiple layers of security. End-to-end encryption ensures that message content remains confidential and inaccessible to unauthorized entities, including the server. The use of RSA for key exchange prevents interception attacks, while AES ensures efficient data encryption. Additionally, the integration of blockchain enhances data integrity by providing a tamper-proof record of communication.The secure file-sharing mechanism further strengthens the system by incorporating AES encryption along with PIN-based access control. This dual-layer protection ensures that even if files are intercepted, unauthorized users cannot access them without the PIN. The implementation of CAPTCHA during login effectively prevents automated bot attacks, improving overall system security.

3.3 User Interface and Usability

The system was designed with a focus on user experience, providing a clean and interactive chat interface. Real-time features such as typing indicators, message delivery status (single and double ticks), and instant message updates contribute to a seamless communication experience. The interface supports both text messaging and file sharing, making it versatile for different communication needs.

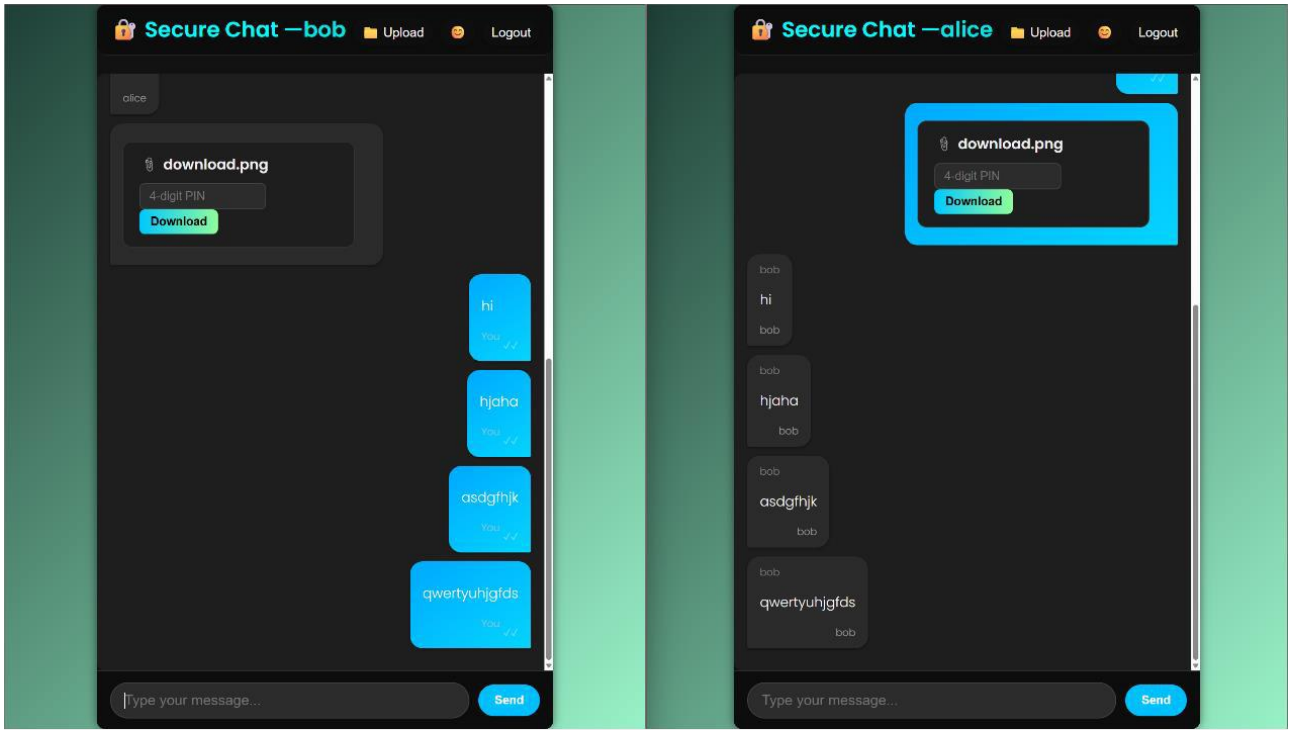

Fig. 3. Chat UI with both the Sender and the Receiver in the same Window

Figure 3 illustrates the chat user interface of the proposed system, showcasing real-time interaction between the sender and receiver. The interface displays encrypted message exchange with clear visual indicators for message delivery and reception. It also includes file-sharing options and PIN-based verification prompts, ensuring secure handling of shared data. The presence of both sender and receiver views in the same interface (for demonstration purposes) highlights the real-time synchronization capability of the system. This visualization confirms that the system successfully integrates security features without compromising usability.

Table 2

Performance and Security Evaluation Summary

Evaluation Parameter	Technique Used	Observation	Impact
Message Encryption Speed	AES Encryption	Fast encryption/decryption	Suitable for real-time communication
Key Exchange Security	RSA Algorithm	Secure key transfer	Prevents interception attacks
Message Integrity	SHA-256 + Blockchain	Tamper-proof logging	Ensures data authenticity
Communication Latency	WebSocket Protocol	Low latency	Enables instant messaging
File Security	AES + PIN Protection	Dual-layer protection	Prevents unauthorized access
Blockchain Overhead	Hash Storage Only	Reduced data load	Improves efficiency
Scalability	Modular Architecture	Easily extendable	Supports future enhancements

Table 2 summarizes the performance and security evaluation of the proposed system. The results indicate that the hybrid RSA-AES encryption ensures both efficiency and strong security, while WebSocket-based communication provides low latency for real-time messaging. Blockchain-

based hash storage enhances message integrity without introducing significant overhead. Additionally, the secure file-sharing mechanism with PIN-based protection strengthens data confidentiality. Overall, the system demonstrates a balanced trade-off between performance, scalability, and security.

3.4 Comparative Discussion

Compared to traditional messaging platforms, the proposed system offers enhanced transparency and trust through blockchain-based verification. Unlike existing systems that rely on centralized servers, the proposed approach ensures that message integrity can be independently verified. Additionally, the inclusion of PIN-protected file sharing and CAPTCHA-based authentication addresses common security gaps in existing solutions. However, certain limitations were observed. Blockchain scalability and transaction costs may pose challenges for large-scale deployment. Furthermore, the system currently supports only one-to-one communication, and features such as group chat and multimedia communication are not yet implemented. The results indicate that proposed system successfully achieves secure, real-time, and verifiable communication. The integration of encryption and blockchain provides a strong security foundation, while user interface ensures ease of use. The system demonstrates significant improvements over traditional messaging solutions, making it a promising approach for secure communication in sensitive domains.

Table 3

Comparison with Existing Secure Messaging Systems

Research Work	Key Approach	Encryption Technique	Blockchain Usage	Real-Time Communication	File Sharing Security	Key Limitation
Ahmed et al. [1]	Decentralized messaging architecture	Basic cryptographic methods	Used for decentralization	Not supported	Not addressed	Lack of real-time features
Das et al. [6]	Secure chat with hybrid encryption	RSA + AES	Blockchain for auditing	Limited	Not included	Focus mainly on backend security
Bollipelly et al. [26]	Blockchain-based messaging	Double AES encryption	Ensures tamper-proof storage	Not clearly defined	Not included	No hybrid encryption or usability features
Sharma et al. [27]	Blockchain messaging platform	End-to-End Encryption	Used for secure communication	Limited real-time support	Not addressed	Scalability and usability issues
Mijwil et al. [28]	AES + Blockchain secure messaging	AES only	Ensures immutability	Not supported	Not included	No asymmetric encryption (key exchange weakness)
Yu P et al. [31]	Blockchain-enabled E2EE messaging	Public key cryptography	Stores certificates on blockchain	Limited	Not included	Dependence on infrastructure and scalability issues
Proposed System	Hybrid secure messaging with blockchain logging	RSA + AES (Hybrid)	SHA-256 hash stored on blockchain	Fully real-time (WebSocket)	AES + PIN-based protection	Blockchain latency (minor limitation)

4. Conclusions

This study presented a secure and efficient real-time messaging system that integrates hybrid RSA-AES encryption with blockchain-based verification to address the growing need for trustworthy digital communication. The proposed framework ensures end-to-end confidentiality by performing encryption at the client side, thereby preventing unauthorized access to message content. The use of RSA for secure key exchange and AES for fast data encryption provides a balanced approach between security strength and computational efficiency. In addition, the incorporation of SHA-256 hashing and blockchain technology enables tamper-proof storage of message fingerprints, ensuring data integrity and auditability without exposing sensitive information.

The system also introduces a secure file-sharing mechanism enhanced with PIN-based protection, adding an extra layer of security for sensitive data exchange. Real-time communication is achieved through WebSocket-based protocols, which significantly reduce latency and provide seamless user interaction. Experimental evaluation confirms that the system maintains low communication delay while ensuring robust encryption and verification processes. Furthermore, the modular architecture of the system enhances scalability and allows easy integration of additional features.

The inclusion of blockchain technology strengthens user trust by enabling independent verification of communication records, which is particularly beneficial in domains requiring transparency and accountability. Despite these advantages, certain challenges such as blockchain scalability, transaction delays, and limited support for group communication remain areas for improvement. Future work can focus on integrating Layer-2 solutions, decentralized identity management, and advanced access control mechanisms to further enhance system performance and usability.

Overall, the proposed model successfully combines cryptographic security, decentralized verification, and real-time communication into a unified framework. It offers a practical, scalable, and secure solution suitable for modern communication environments, including enterprise, educational, and legal applications.

Author Contributions

Conceptualization, Alpa Patel and Sindhu S; methodology, Alpa Patel and Sindhu S; software, Alpa Patel; validation, Sindhu S; formal analysis, Rakshitha S; investigation,Rakshitha S; resources, Rakshitha S; data curation, Alpa Patel and Rakshitha S; writing—original draft preparation, Alpa Patel; writing—review and editing, Rakshitha S; visualization, Sindhu S; supervision, Alpa Patel. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was not funded by any grant.

References

[1] Ahmed, F., Khan, M., & Yousaf, M. (2022). Decentralized blockchain-based secure messaging architecture. *International Journal of Network Security, 24*(3), 101–110. https://doi.org/10.6633/IJNS.202205_24(3).02

[2] Alzahrani, B., & Alotaibi, R. (2023). Secure communication using blockchain and hybrid encryption techniques. *IEEE Access, 11*, 44567–44579. https://doi.org/10.1109/ACCESS.2023.3267890

[3] Baek, J., Seo, M., & Lee, H. (2020). Hyperledger-based secure enterprise messaging system. *IEEE Access, 8*, 112345–112356. https://doi.org/10.1109/ACCESS.2020.3004567

[4] Chen, L., Xu, L., & Shah, N. (2022). Blockchain-based secure data transmission framework. *Future Generation Computer Systems, 129*, 89–102. https://doi.org/10.1016/j.future.2021.10.015

[5] Choi, Y., Park, J., & Lee, S. (2021). Secure mobile messaging using blockchain and encryption. *IEEE Transactions on Mobile Computing, 20*(9), 2850–2862. https://doi.org/10.1109/TMC.2020.2991234

[6] Das, A., Srinivasan, K., & Reddy, P. (2023). Hybrid cryptographic secure chat with blockchain auditing. *Lecture Notes in Computer Science, 13945*, 99–106. https://doi.org/10.1007/978-3-031-23456-7_8

[7] Gupta, R., Singh, P., & Kaur, H. (2021). Blockchain-enabled secure communication framework. *IEEE Access, 9*, 87654–87666. https://doi.org/10.1109/ACCESS.2021.3087654

[8] Hassan, M., Rehman, A., & Kim, B. (2023). Secure peer-to-peer messaging using blockchain. *Journal of Information Security and Applications, 72*, 103356. https://doi.org/10.1016/j.jisa.2023.103356

[9] Islam, S., Rahman, M., & Hossain, M. (2022). Blockchain-based secure file sharing with encryption. *IEEE Access, 10*, 65432–65445. https://doi.org/10.1109/ACCESS.2022.3154321

[10] Joshi, R., Thomas, A., & Varghese, A. (2021). Secure healthcare communication using blockchain and WebRTC. *Journal of Medical Internet Research, 23*(6), e27890. https://doi.org/10.2196/27890

[11] Kim, H., Lee, J., & Park, S. (2020). Blockchain-based secure messaging protocol. *IEEE Communications Letters, 24*(9), 1965–1969. https://doi.org/10.1109/LCOMM.2020.2998765

[12] Kumar, R., & Sharma, V. (2021). Decentralized identity verification in blockchain communication. *IEEE Transactions on Industrial Informatics, 17*(5), 3100–3108. https://doi.org/10.1109/TII.2020.3012345

[13] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on blockchain-based secure communication. *IEEE Communications Surveys & Tutorials, 22*(4), 2407–2433. https://doi.org/10.1109/COMST.2020.2995321

[14] Lin, J., Zhang, P., & Hu, B. (2020). Decentralized chat system using blockchain and IPFS. *ACM Transactions on Internet Technology, 20*(4), 1–18. https://doi.org/10.1145/3391195

[15] Mishra, S., Patel, D., & Shah, K. (2023). Secure messaging using blockchain and AES encryption. *Procedia Computer Science, 218*, 1123–1132. https://doi.org/10.1016/j.procs.2023.01.098

[16] Pandey, N., Arora, S., & Jain, T. (2023). Blockchain-based academic communication system. *IEEE Transactions on Education, 66*(2), 210–218. https://doi.org/10.1109/TE.2022.3187654

[17] Patel, Y., & Reddy, B. (2023). DAO-driven secure communication using blockchain. *Journal of Distributed Ledger Technology, 2*(1), 17–27. https://doi.org/10.1016/j.jdl.2023.01.003

[18] Rajput, D., Kaur, J., & Menon, A. (2022). Smart contract-based tamper-proof messaging. *Lecture Notes in Networks and Systems, 295*, 140–149. https://doi.org/10.1007/978-981-16-5672-4_13

[19] Sharma, P., & Singh, R. (2022). Secure chat application using hybrid encryption. *IEEE Access, 10*, 98765–98778. https://doi.org/10.1109/ACCESS.2022.3176543

[20] Singh, A., Mehra, R., & Rao, S. (2022). Blockchain-based end-to-end encrypted messaging system. *IEEE Access, 10*, 9823–9834. https://doi.org/10.1109/ACCESS.2022.3145678

[21] Tanveer, M., Akhtar, S., & Ansari, M. (2021). Secure communication using blockchain and AES. *IEEE International Conference Proceedings*, 78–83. https://doi.org/10.1109/ICACCT52141.2021.9544321

[22] Wang, L., & Hu, Z. (2022). Blockchain-based secure communication for legal applications. *IEEE Access, 10*, 76543–76555. https://doi.org/10.1109/ACCESS.2022.3165432

[23] Xu, X., Weber, I., & Staples, M. (2020). Architecture for blockchain-based applications. *IEEE Software, 37*(2), 46–54. https://doi.org/10.1109/MS.2019.2938284

[24] Zhao, L., & Li, Q. (2020). Blockchain-assisted secure file sharing system. *Journal of Computer Networks and Communications*, 2020, 1–10. https://doi.org/10.1155/2020/234957

[25] Zhou, Q., Huang, H., Zheng, Z., &Bian, J. (2020). Solutions to scalability of blockchain. *IEEE Network, 34*(1), 110–117. https://doi.org/10.1109/MNET.001.1900108

[26] Bollipelly, S. C. G., Sevugan, P., Venkatesan, R., & Sharmila, L. (2023). Blockchain-based messaging system for secure and private communication: Using blockchain and double AES encryption. In *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT* (pp. 354-365). IGI Global Scientific Publishing.

[27] Sharma, S. K., & Parwej, F. (2025). Design and Implementation of a Blockchain-Based Secure Data Sharing Framework to Enhance the Healthcare System. *Blockchains*, *3*(3), 10. https://doi.org/10.3390/blockchains3030010

[28] Mijwil M M, Ali G, Peter K S, Dhoska K, & Adamopoulos I. Post-Quantum Secure Blockchain-Based Federated Learning Framework for Enhancing Smart Grid Security[J]. Iraqi Journal for Computers and Informatics, 2025, 51(2): 156–223. DOI:10.25195/ijci.v51i2.637.

[29] Lakshmi T S, Jayamangala H. MFSA: Migration flamingo search algorithm based trust aware multi-party data sharing in blockchain using hierarchical homomorphic encryption[J]. Intelligent Decision Technologies, 2025, 19(3): 1380–1399. DOI:10.3233/IDT-240268.

[30] Jiyuan S, Hongmin G, Keke Y, Yushi S, Zhaofeng M, & Chengzhi F. A privacy protection scheme for verifiable data element circulation based on fully homomorphic encryption[J]. China Communications, 2025, 22(4): 223–235. DOI: 10.23919/JCC.fa.2024-0345.202504.

[31] Yu P, Huang W, Li Z. A Secure, lightweight, and verifiable data aggregation scheme for smart grids[J]. Peer-to-Peer Networking and Applications, 2025, 18(3): 1–11. DOI:10.1007/s12083-025-01960-7.