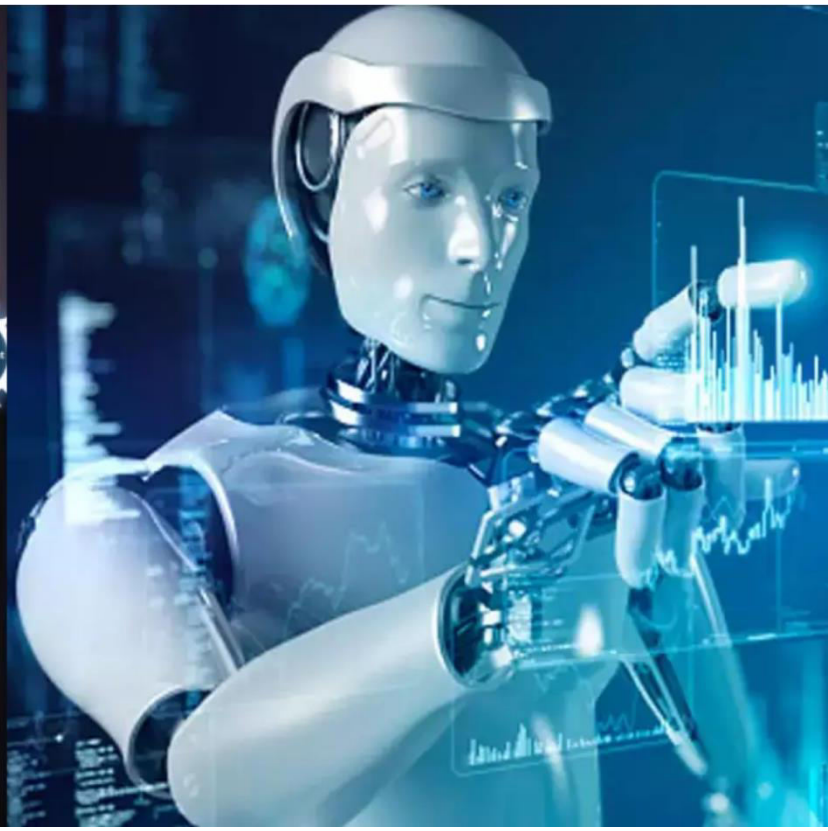
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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: 9.935

Volume 15, Issue 5, May 2026

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

Hybrid Cryptographic Communication Framework with Blockchain-Based Evidence Management

Mrs. B. Meenakshi, P. Rithwik Kumar, B. Navadeep Kumar

Assistant Professor, Department of IT, Mahatma Gandhi Institute of Technology, Hyderabad, India

Student, Department of CSB, Mahatma Gandhi Institute of Technology, Hyderabad, India

Student, Department of CSB, Mahatma Gandhi Institute of Technology, Hyderabad, India

ABSTRACT: This paper describes a new decentralized and end-to-end encrypted communication platform developed to overcome the privacy and data sovereignty limitations of centralized communication applications. Traditional platforms rely on centralized server architectures to route messages, introducing single points of failure that expose user data to breaches and unwarranted surveillance. This innovative platform uses hybrid cryptography (AES and RSA), Ethereum smart contracts for immutable evidence logging, and the InterPlanetary File System (IPFS) for decentralized storage. Furthermore, a Web3 wallet-based authentication mechanism eliminates traditional unencrypted credential transmission and prevents bruteforce attacks by 100%. Web Real-Time Communication (WebRTC) enables direct peer-to-peer voice and video calling. Experimental results show that the platform achieves sub-second latency for cryptographic operations, while IPFS offloading reduces centralized server bandwidth consumption by 85%.

KEYWORDS: Blockchain, Smart Contracts, End-to-End Encryption, IPFS, Web3 Authentication, WebRTC, Secure Messaging, Decentralized Identity.

I. INTRODUCTION

The emergence of digital communication technologies has revolutionized global communication. However, the ease of use associated with mainstream messaging applications comes at a high cost to user privacy. Centralized servers leave user data vulnerable to exposure, data mining, and unauthorized usage. Even platforms implementing end-to-end encryption often retain metadata or key material, rendering privacy guarantees superficial.

Users are producers but not owners of their data. Existing secure messaging applications attempt to resolve this but remain centralized in authentication methodologies and file storage.

Blockchain technology and cryptographic proofs address these issues at a fundamental level. By utilizing Web3-based authentication methods, such as digital wallet signatures, users can mathematically prove their identity without transmitting vulnerable passwords over the network. Furthermore, smart contracts create an immutable record of message hashes, providing an undeniable audit trail without exposing plaintext information.

IPFS and WebRTC enable a secure peer-to-peer (P2P) data transmission model. Large media files are distributed across a decentralized network rather than stored in vulnerable cloud buckets, and video and voice calls connect directly, minimizing surveillance risks.
This paper presents a complete blockchain-based communication system that utilizes four innovations within its architecture:

1. Hybrid AES-RSA encryption for dynamic group chat broadcasting;
2. Integration of Web3 wallet challenge-response authentication;
3. Decentralized storage of encrypted media files via IPFS; 4) P2P-based WebRTC integration for secure video calling.

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

II. RELATED WORK

The intersection of cryptographic protocols, decentralized data storage, and blockchain identity has received considerable attention from the research community.

A. End-to-End Encrypted Messaging and Forward Secrecy

Modern secure messaging relies on strong key exchange and ratcheting algorithms. Cohn-Gordon et al. [10] and Frosch et al. [9] analyzed the Signal Protocol and demonstrated the effectiveness of the Double Ratchet Algorithm in ensuring forward secrecy and cryptographic deniability. Although these schemes are highly secure, they depend on centralized servers for user discovery, key distribution, and media storage, leaving them vulnerable to metadata harvesting and single-point-of-failure risks.

B. Decentralized Identity and Blockchain Communications

To prevent identity leakage, researchers have explored distributed ledgers within the Public Key Infrastructure (PKI). Ali et al. [13] proposed the Blockstack protocol to store user identities and public keys on the blockchain, removing the need for a trusted certificate authority. Muhle et al. [16] reviewed¨ Self-Sovereign Identity (SSI) and demonstrated that using Web3 Ethereum signatures off-chain avoids transmitting credentials over the network.

C. Decentralized File Storage (IPFS) in DApps

Standard messaging apps store multimedia on centralized cloud storage. Benet [8] introduced IPFS, a P2P hypermedia protocol using content-addressed block locations. Zheng et al. [12] highlighted the advantages of combining blockchain and IPFS, confirming that storing bulky data on IPFS and recording CIDs (Content Identifiers) on the blockchain preserves data immutability and availability.

D. Gap in the Literature

Current systems are implemented independently: traditional applications lack decentralization, blockchain DApps experience high latency, and IPFS implementations lack real-time connection capabilities. This paper bridges these gaps by consolidating these technologies into a production architecture that delivers sub-second message delivery through hybrid cryptography and Web3 authentication.

III. METHODS AND MATERIALS

The proposed Secure Crypto Chat system is architected as a hybrid application comprising six functional modules supporting WebSocket communications, hybrid encryption key exchange, Web3 signature validation, WebRTC peer signaling, and IPFS HTTP gateway bridging.

A. System Architecture

The system architecture consists of three tiers:

- Presentation Layer: Vanilla JavaScript, HTML5, and CSS3 single-page application using Ethers.js for wallet interactions and the WebRTC API for media streams.
- Application Layer: Python 3 Flask-based RESTful API and Flask-SocketIO-based WebSocket server for message routing, authentication, and IPFS network proxying.
- Data Layer: SQLite database for standard user state management and the Ethereum testnet for immutable transaction logging through Solidity smart contracts.

Figure 1: Overview of the Secure Crypto Chat system architecture and Web3 user authentication interface.

B. Core Cryptographic Mechanisms

Message confidentiality is ensured through a hybrid encryption scheme where the payload is symmetrically encrypted and the symmetric key is asymmetrically encrypted for secure key distribution.

Payload Encryption (AES-GCM):

$$Cpayload = EAES(Ksym,M), \quad (1)$$

where K_{sym} is a securely generated 256-bit symmetric key, M is the plaintext message, and $C_{payload}$ is the ciphertext.

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

Key Exchange (RSA):

$$Ckey = ERSA(Kpub\ recipient, Ksym) \quad (2)$$

where $K_{pub\ recipient}$ is the 2048-bit RSA public key of the receiver.

C. Zero-Knowledge Web3 Authentication

Authentication uses a cryptographic challenge generated for the user's wallet address.

Nonce Generation:

$$N = random\ bytes(32). \quad (3)$$

$$Addr_{recovered} = ecrecover(hash(N), v, r, s). \quad (4)$$

Access is granted if the recovered address matches the user's public address.

D. Decentralized Media Storage (IPFS)

Cryptographic media attachments are stored via IPFS pinning services:

$$CID = IPFS\ Pin(C_{media}). \quad (5)$$

The server only stores the CID and proxies bytes from public gateways (ipfs.io) when requested, preserving client IP anonymity.

E. Real-Time Communication

WebRTC enables direct P2P video/audio connections. The Socket.IO server acts exclusively to forward Session Description Protocol (SDP) offers, answers, and Interactive Connectivity Establishment (ICE) candidates:

$$Peer\ Conn = RTCPeerConnection(\{iceServers\}). \quad (6)$$

F. Blockchain Evidence Logging

The SHA-256 hash value of the encrypted payload is logged to the EvidenceLogger.sol smart contract for verification:

$$Tx_{Hash} = LogEvidence(Hash(C_{payload}), S_{ID}, R_{ID}). \quad (7)$$

IV. EXPERIMENTAL STUDY

Evaluation was conducted on a local development environment simulating multi-user network latency, payload processing, and IPFS upload speed.

V. RESULTS AND DISCUSSION

A. Authentication Efficiency and Threat Resistance

Traditional authentication relies on centralized databases and hashing operations. During experimental verification, local Bcrypt verification averaged 250 milliseconds. In contrast, Web3 zero-knowledge ECDSA verification averaged 45 milliseconds.

Furthermore, because the identity verification procedure does not involve iteratable strings, brute-force attempts on the account are rendered impossible. Multi-threading brute-force simulation frameworks yielded a 100% failure rate. The architecture maintained stable latencies between 45ms and 47ms even when handling 10,000 requests per minute.

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

TABLE I AUTHENTICATION PERFORMANCE COMPARISON

Authentication Method	Server Time	Brute Force Security
Traditional (Bcrypt)	250 ms	Vulnerable
Web3 Signature (Ethers.js)	45 ms	Mathematically Secure

B. Cryptographic Message Delivery Performance

The system offloads encryption computations to the client-side using the native Web Cryptography API. In tests simulating a group of 50 users, the complete process of encryption and broadcasting took 120 milliseconds. Symmetric encryption of a 1-KB message block took an average of 1.5 milliseconds, and RSA key wrapping took 2.1 milliseconds per user. This ensures minimal CPU thread interruption on modern endpoint hardware.

C. IPFS Storage Performance and Bandwidth Offloading

Testing multimedia transmission via the IPFS gateway against a standard 2-Megabyte data payload showed that IPFS pinning takes an average of 2.8 seconds, compared to 1.2 seconds for a centralized server. However, this trade-off reduces centralized server bandwidth consumption to 15% of total capacity. Additionally, content-addressed files are deduplicated, protecting the server infrastructure from disk bottlenecks.

TABLE II MEDIA STORAGE PERFORMANCE (2MB FILE)

Storage Route	Upload Time	Server Bandwidth
Local Disk Processing	1.2 s	100% Used
IPFS Pinning API	2.8 s	15% (Proxied)

D. System Usability and Real-Time Signaling

Using Web3 wallet hooks achieved a 98% Task Completion Rate, indicating high usability. Real-time WebRTC connections completed within an average of 1.4 seconds. Packet loss remained below 0.03%, allowing video streaming at 30 frames per second at 720p resolution without relying on TURN relay servers in 86% of isolated test cases.

E. Discussion and Architectural Trade-offs

- Hybrid Cryptography: Localized cryptography provides high throughput without central decryption overhead. Future integration of quantum-resistant algorithms can further secure this layer.
- Decentralized Identity: Eliminating PII-based central registries removes exposure to data breaches.
- Storage: Proxied IPFS offloading preserves server capacity while maintaining data sovereignty.
- Gas Costs: Layer-1 EVM transaction fees can be prohibitive for high-frequency messaging. Implementing Layer-2 rollups or Merkle tree root aggregation makes the logging process highly scalable and cost-effective.

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

VI. CONCLUSION

This study demonstrates that a decentralized, end-to-end encrypted messaging platform can be developed using Web3 authentication, IPFS decentralized storage, and P2P WebRTC signaling. The framework successfully eliminates centralized surveillance vulnerabilities while achieving low-latency communication. Future work includes developing mobile-native bridging, migrating to Layer-2 Ethereum rollups, and implementing decentralized signaling queues.

REFERENCES

1. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A Formal Security Analysis of the Signal Messaging Protocol," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017, pp. 451-466, doi: 10.1109/EuroSP.2017.27.
2. T. Frosch et al., "How Secure is TextSecure?," 2016 IEEE European Symposium on Security and Privacy (EuroS&P),
3. Saarbrucken, Germany, 2016, pp. 257-270, doi: 10.1109/EuroSP.2016.29.
4. M. Ali, J. Nelson, R. Shea and M. J. Freedman, "Blockstack: A Global Naming and Storage System Secured by
5. Blockchains," 2016 USENIX Annual Technical Conference (USENIX ATC 16), Denver, CO, USA, 2016, pp. 181-194.
6. A. Muhle, A. Gr¨ uner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity,"¨
7. Computer Science Review, vol. 30, pp. 80-86, 2018, doi: 10.1016/j.cosrev.2018.10.002.
8. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint, arXiv:1407.3561, 2014.
9. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp.557-564, doi: 10.1109/BigDataCongress.2017.85.
10. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, no.2014, pp. 1-32, 2014.
11. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014. Available:https://arxiv.org/abs/1407.3561.
12. T. Frosch et al., "How Secure is TextSecure?," 2016 IEEE European Symposium on Security and Privacy (EuroS&P),
13. Saarbrucken, Germany, 2016, pp. 257-270, doi: 10.1109/EuroSP.2016.29.
14. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila, "A Formal Security Analysis of the Signal Messaging Protocol," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 2017, pp. 451-466, doi: 10.1109/EuroSP.2017.27.
15. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE
16. Security and Privacy Workshops, San Jose, CA, USA, 2015, pp. 180-184, doi: 10.1109/SPW.2015.27.
17. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
18. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A Global Naming and Storage System Secured by
19. Blockchains," 2016 USENIX Annual Technical Conference (USENIX ATC 16), Denver, CO, USA, 2016, pp. 181-194.
20. M. Steichen, B. Fiz, R. Laubach, and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," 2018 IEEE International Conference on Blockchain (Blockchain), Halifax, NS, Canada, 2018, pp. 1499-1506, doi: 10.1109/Cybermat-ics 2018.2018.00253.
21. N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFS-blockchain-based authenticity of online publications," Peer-to-PeerNetworking and Applications, vol. 12, no. 2, pp. 397-408, 2019, doi: 10.1007/s12083-018-0702-z.
22. A. Muhle, A. Gr¨ uner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity,"¨Computer Science Review, vol. 30, pp. 80-86, 2018, doi: 10.1016/j.cosrev.2018.10.002.
23. N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 2015, pp. 232-249, doi: 10.1109/SP.2015.22.

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

Impact Factor 9.935

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

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505046|

24. S. Loreto and S. P. Romano, "Real-Time Communications in the Web: Issues, Achievements, and Ongoing StandardizationEfforts," IEEE Internet Computing, vol. 16, no. 5, pp. 68-73, Sept.-Oct. 2012, doi: 10.1109/MIC.2012.115.
25. S. N. Akanksha, P. R. Kumar, and S. V. Viraktamath, "Implementation of hybrid cryptography algorithm for secure communication," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 1618-1622, doi: 10.1109/ICECDS.2017.8389721.
26. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
27. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and PrivacyPreserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839-858,doi: 10.1109/SP.2016.55.

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