International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

Security and Resilience in Decentralized P2P Communication

Kanu Priya Mittal[1]; Dr. Naveen Chandra[2]

[1,2]Department of Computer Application, Swami Vivekanand Subharti University Meerut, India

Email: kanupriyamittalmzn@gmail.com

Abstract

Noteworthy issues about privacy, parallelism, resilience, and centralised control have been brought up by the growing reliance on real-time digital communication systems. The centralized client-server designs used by the majority of modern messaging systems disclose communication metadata, create single points of failure, and constrain user faith in service providers. With a focus on P2P-first architectures, end-to-end encryption, decentralised trust mechanisms, group communication stability, and adaptive cloud-based fallback mechanism, this review methodically investigates research on secure decentralised peer-to-peer (P2P) communication systems. A thorough analysis is conducted of key enabling technologies, such as WebRTC, Conflict-Free Replicated Data Types (CRDTs), blockchain-based identity frameworks, and selective cloud support. In order to create reliable, scalable, and privacy-preserving real-time communication systems appropriate for next-generation applications, the review reveals major gaps, outlines existing research, and suggests future research areas.

Keywords

Peer-to-Peer Communication; Decentralized messaging; End-to-End Encryption; CRDT; Blockchain; Cloud Assisted Fallback; NAT Traversal; Decentralized Architecture; WebRTC; Metadata Privacy; Distributed Systems.

1. Introduction

Digital communication systems, being able to facilitate two-way interaction in personal, professional, live, immediate connectivity for work itself, have been an unavoidable part of modern civilization's evolution today. Major communication platforms across the globe, most popular platforms like Telegram, Instagram, iMessage, Facebook Messenger, Signal or WhatsApp and Discord. Irrespective of their success, these systems are typically based on centralized designs, where servers are facilitated functioning like storage, synchronization, message routing, facilitating communication and managing network resources on central servers.

While unified centralized framework for system management and coordination can be easy to design, they indispensable have some limitations. The central servers are criticized for outages, censorship and surveillance and also have had immense data leaks as they are single points of failures. Although end-to-end encryption (E2EE) is widely used to protect the content of messages, metadata such as identities, timing, contextual information and frequency are disclosed. In this interpretation, in

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

contemporary communication systems, a clear divergence has emerged between the protection of content and that of metadata. These limitations have inspired the study of decentralised peer-to-peer (P2P) communication models that reduces the dependence on central servers. P2P systems can better distribute each node control and responsibility by requiring direct communicating user communication.

The main objectives of a communication network are to transmit a message, such as a data stream from a transmitter by radio waves, and to deliver it either precisely or in close proximity to a recipient. This section concentrates on a particular layer of the Open Systems Interconnection (OSI) model. The ordinary communication framework separates signal processing into a sequence of multiple independent units at both the transmitter and receiver, improving each unit individually for varying utility. It implements various deep learning principles for a communication system. Decentralized networks provide multiple benefits; however, as these networks develop, many nodes become either actively or passively unreachable due to Network Address Translation (NAT) or firewall settings. The challenge in accessing these nodes poses a major barrier to the advancement of decentralized networks, as it interrupts data exchange between nodes that are unreachable. This complication is prevented in various applications, including decentralized file storage systems, decentralized social media networks, and decentralized Internet of Things (IoT) infrastructures.

2. Literature Review

Early research in P2P security focused on cryptographic techniques such as encryption, digital signatures, and hash functions to ensure confidentiality and integrity. While effective, these methods do not address trust issues among nodes.

Trust management systems were later introduced to evaluate node behavior and establish reputation-based communication. These systems improve reliability but are vulnerable to manipulation and collusion attacks.

Blockchain technology has emerged as a promising solution by providing decentralized trust through consensus mechanisms. It ensures data integrity and transparency but suffers from scalability and latency issues.

Machine learning and AI-based approaches have recently been applied to detect anomalies and malicious activities in P2P networks. Techniques such as anomaly detection, clustering, and deep learning improve detection accuracy but require high computational resources.

Overall, existing literature indicates that no single approach is sufficient, highlighting the importance of hybrid solutions combining multiple security paradigms.

We presented WebRTC Swarms, a novel architecture for decentralized, privacy preserving signaling and group authorization in peer-to-peer networks. By integrating onion-routed relay circuits with zero-knowledge membership proofs and cryptoeconomic incentives, our design achieves a synergy between privacy, security, and sustainability that is greater than the sum of its parts. Users discover and connect to peers without exposing identities or IP addresses, relying on an overlay of incentivized full nodes to carry signaling traffic.

3. Proposed Methodology

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

The proposed methodology focuses on designing and analysing a secure and resilient decentralized peer-to-peer (P2P) communication framework that reduces dependency on centralized servers while maintaining privacy, scalability, and reliable real-time communication. The methodology is divided into multiple stages to systematically evaluate existing technologies and integrate them into a unified communication architecture.

Initially, an appropriate literature survey is conducted using authentic research sources such as IEEE Xplore, SpringerLink, Google Scholar, Scopus, research journals, conference papers, and open-source technical repositories. The collected studies are examined to understand the strengths and limitations of centralized messaging systems, decentralized communication architectures, encryption models, consistency management techniques, and adaptive cloud-assisted solutions. The review mainly concentrates on peer-to-peer and decentralised communication systems, collaboration and instant messaging systems, security and privacy mechanisms, for example decentralised trust and end-to-end encryption, methods for ensuring coherence between group communications, hybrid and cloud-assisted communication models.

After collecting the relevant literature, a comparative analysis approach is applied to classify the selected studies according to their architectural model, communication protocol, security mechanism, and infrastructure dependency. The analysis identifies how centralized systems rely heavily on servers for routing, synchronization, and metadata management, whereas decentralized systems distribute communication responsibilities among participating peers. Thematic analysis was performed to categorize the studies based on architectural design, security approach, consistency mechanism, and infrastructure dependency. This systematic approach allows us to focus on research gaps, and to logically compare existing or present solutions.

The proposed framework adopts a P2P-first communication architecture in which users communicate directly without continuous dependence on central servers.With its standard approach to discovering peers, making safe connections and exchanging low-latency data, WebRTC has been a game changer for real-time P2P communication. However, in reality, the practical deployment of WebRTC-based systems is hindered by NAT traversal and firewall limitations; often requiring relay servers that partially return to a centralized model,the methodology incorporates selective cloud-assisted fallback services that are activated only when direct peer connectivity fails. This hybrid strategy reduces infrastructure overhead while preserving decentralization as much as possible.

For security and privacy, the methodology integrates end-to-end encryption (E2EE) to ensure that only intended users can access communication content. In addition, decentralized identity validation techniques based on blockchain-inspired trust models are examined to eliminate excessive reliance on centralized authentication authorities. Instead of using blockchain for full message transmission, it is selectively utilized for identity verification, cryptographic key management, and trust establishment between communicating peers. This approach improves transparency and tamper resistance while avoiding the scalability limitations associated with blockchain-heavy systems.

To maintain synchronization and consistency during group communication, the methodology studies the use of Conflict-Free Replicated Data Types (CRDTs). CRDT mechanisms allow distributed nodes to update shared communication states concurrently without causing synchronization conflicts. These mechanisms are particularly useful in decentralized messaging environments where users may operate across unstable or heterogeneous networks. The methodology also evaluates the computational and storage overhead introduced by CRDT implementations in real-time systems.

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

The final phase of the methodology involves evaluating the proposed hybrid architecture on the basis of privacy preservation, fault tolerance, scalability, communication latency, infrastructure dependency, and reliability. Existing decentralized and centralized communication approaches are comparatively analysed to determine how adaptive fallback mechanisms, decentralized trust models, and consistency management techniques can be integrated into a practical next-generation communication framework. The methodology ultimately aims to provide a balanced communication model that combines the resilience and privacy advantages of decentralization with the operational reliability of selective cloud support.

4. Communication Protocol Evolution and Privacy Implications

1. Client–Server Paradigm and TCP-Based Communication

Client-server type, centralised architectures provided a simple to implement and administer alternative for early digital-based messaging systems. Servers in those overlay networks are responsible for user identification, the storage of global state information and providing a guaranteed message ordering on top of an unreliable network. Garg and Müller (1993) Communication protocols based on TCP often over HTTPS or WebSockets, are the foundation of the majority of centralized platforms . While TCP ensures the in order delivery and reliable transfer of messages, high levels of concurrence may lead to delay and performance problems. By multiplexing and persistent connections, we can wring more responsiveness out of it, but also continue to bandage around a centralising dependency. However, as Wang, Sun, and Zhou (2022) demonstrated, TCP's congestion control and retransmission mechanisms introduce measurable latency in high-concurrency real-time applications, particularly when messages traverse multiple server layers.

2. WebSocket and HTTP/2 Enhancements

The introduction of WebSockets represented a significant improvement in communication interactivity. By enabling persistent, full-duplex communication between clients and servers, WebSockets substantially reduced connection establishment overhead compared to traditional HTTP polling. Xu, Chen, and Wang (2023) demonstrated measurable responsiveness improvements in WebSocket-based messaging systems. Nonetheless, this architectural enhancement did not alter the fundamental centralization of communication control; servers remained responsible for managing connection state, routing logic, and access permissions.

HTTP/2 advanced protocol-level efficiency further through multiplexing, header compression, and improved flow control mechanisms. Zhang, Li, and Ren (2021) confirmed that HTTP/2 reduces bandwidth consumption and connection overhead in high-traffic messaging environments. However, empirical evaluation consistently indicates that HTTP/2 does not structurally alter centralized communication architectures—servers remain unavoidable trust anchors in the communication chain.

3. End-to-End Encryption and Residual Privacy Limitations

End-to-end encryption (E2EE) emerged as a major advancement in protecting message content from unauthorized access, including by service providers themselves. Frosch et al. (2021) Secrecy of messages is just one component of security in distributed communication systems. On their side, decentralised settings also need to address authentication, identity management and trust building,

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

along with impersonation resistance as well as the defence against Sybil attacks - despite that E2EE ensures that only the intended recipients are able to access messages content. Despite these advances, E2EE does not eliminate all privacy exposures. Parker and Riva (2022) demonstrated that centralized messaging systems continue to collect and process extensive metadata, including communication timestamps, participant identifiers, message frequency, and network behavioral patterns. Such metadata, independent of message content, can be leveraged to infer sensitive social relationships, behavioral routines, and institutional affiliations. Anderson, Berg, and Feamster (2022) Privacy concerns are one of the biggest dangers of centralised systems. Servers can see metadata even while the content is encrypted with end-to-end encryption (E2EE). It is inherently difficult for centralised servers to provide absolute privacy and, as multiple works demonstrate, revealing sensitive details of social network interactions and user's activities is still possible through analysing metadata.

5. Peer-to-Peer Communication: Principles, Technologies, and Constraints

1. Foundations of Peer-to-Peer Networking

P2P communication systems transmit messages immediately and have reduced latency by not relying on trusted third-party intermediaries, but rather distributing the communication functions between participating nodes. In such architectures, each node may simultaneously function as client and server, sharing responsibility for data exchange, peer discovery, and system maintenance. Zhou, Sun, and Zhang (2025) emphasized that this decentralisation contributes to scalability of the system, reduced dependency on infrastructure and features fault tolerance. The foundational proposition of P2P architectures is that resilience and cost efficiency improve as network responsibility is distributed across end-user devices rather than concentrated in centralized infrastructure.

2. Torrent-Based Systems and Their Relevance to Real-Time Communication

Torrent-based file-sharing networks constitute one of the most extensively studied P2P architectures, demonstrating the feasibility of large-scale decentralized data distribution without centralized servers. These systems pioneered techniques for distributed peer discovery, data chunking, and incentivized sharing that have influenced subsequent decentralized communication research. However, torrent-based systems are one of the first P2P architectures to successfully demonstrate decentralised data delivery. Their focus, though, lies more with bulk and asynchronous transfer of data as opposed to low latency and conversational communication. As Das, Majumdar, and Sen (2023)

3. WebRTC and Real-Time Peer-to-Peer Communication

WebRTC emerged as a standardized framework for real-time P2P communication, providing built-in mechanisms for peer connection establishment, network path negotiation, and media and data exchange. Jennings, Johnston, and Jensen (2021) demonstrated that WebRTC enables latency characteristics suitable for audio, video, and bidirectional data channels, making it a technically promising foundation for decentralized messaging applications. Unlike traditional client–server communication systems, WebRTC permits peers to exchange data directly once a connection has been established, substantially reducing server involvement during active sessions.

A critical limitation of WebRTC in practice is the challenge of traversing network address translation (NAT) boundaries and firewall restrictions. A substantial proportion of end-users operate behind

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

restrictive network configurations that prevent unsolicited inbound connections. Alabi et al. (2020) showed that in such environments, direct peer connections frequently fail, necessitating the deployment of relay servers—specifically TURN servers—to forward traffic between peers. Haque, Islam, and Rahman (2022) further quantified performance trade-offs in WebRTC deployments, finding that relay-mediated communication introduces latency and bandwidth penalties that partially negate P2P efficiency gains.

4. Adaptive Fallback Strategies

The direct communication of P2P is prioritized in adaptive fallback system, and a cloud-based relay service will play its role only when the direct connection cannot be established because of the network problem. Empirical evidence suggests that selective fallback significantly reduces the cost of infrastructure without compromising reliability and quality of service. Both decentralisation and operational resilience are pragmatically combined in this hybrid way. Cao, Li, and Wang (2024) demonstrated that adaptive relay selection strategies significantly reduce relay dependency compared to static configurations, achieving greater overall decentralization without sacrificing connectivity reliability. Rahman, Hasan, and Rahman (2024) further proposed latency optimization techniques for P2P communication that dynamically adjust path selection based on measured network conditions. These findings support a hybrid model in which decentralization is maximized under favorable network conditions while fallback mechanisms ensure service continuity otherwise.

5. Peer Discovery in Decentralized Systems

In centralized systems, servers maintain authoritative directories of user identities and connection states. Decentralized systems must solve the peer discovery problem without such central directories. Distributed hash tables (DHTs), popularized by protocols such as Kademlia, provide structured overlay networks through which peers can locate each other using consistent hashing without central coordination. Gossip-based dissemination protocols, examined by Kermarrec, Massoulie, and Ganesh (2003; 2004), offer probabilistic peer discovery suitable for dynamic network membership. Zhang, Wang, and Chen (2023) evaluated secure peer discovery mechanisms in decentralized networks, identifying trade-offs between discovery efficiency, resistance to Sybil attacks (Douceur, 2002), and metadata exposure through network-level interactions.

6. Consistency Management: Conflict-Free Replicated Data Types

1. The Consistency Challenge in Decentralized Group Communication

In decentralised design, group communication make worse the situation as it involves more difficulties such as message sequences and state accuracy. In centralized systems, messages are sequenced in a correct order by servers ensuring consistent view between users. Even in a decentralised system without central facilitator, maintaining consistency is still very challenging to bridging the gap. Centralized chat systems resolve this challenge trivially: the server imposes a total ordering on all messages, ensuring that all participants observe an identical message sequence regardless of network conditions. In decentralized environments lacking a central coordinator, concurrent message generation across multiple peers can produce divergent local states, undermining the consistency guarantees that users expect from messaging applications. Pietzuch, Shneidman, and Roussopoulos

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

(2020) characterized consistency management as one of the most significant structural obstacles to practical decentralized chat adoption.

2. CRDT Principles and Messaging Applications

One reassuring path to maintaining consistency in distributed systems is offered by CRDTs.CRDTs rectify concurrent updates without requiring complex conflict-resolution logic or manual intervention, often by using mathematical principles or protocols. They are especially suitable for unified and decentralised group communication due to their conceptual assurance. Shapiro, Preguica, Baquero, and Zawirski (2022) provided formal proofs that CRDTs allow distributed nodes to independently apply updates and reach consistent final states regardless of message delivery order or temporary network partitions. This property makes CRDTs theoretically well-suited to decentralized messaging environments where network partitions and asynchronous message delivery are routine.

Baquero and Moura (2020) explored CRDT application to real-time collaborative systems, however, the mathematical approach of CRDT-based systems introduces tradeoffs such as leading to increased storage overhead, computational complexity, low latency and offline-first support. These challenges are particularly prominent in real-time communication, and resource constrained environments where further optimisation by design is needed as well as objective empirical evaluation. Alonso, Kossmann, and Wiesmann (2021) reviewed distributed systems consistency models and confirmed that these overheads present deployment challenges for high-throughput, real-time messaging scenarios. Zhang, Hu, and Chen (2024) subsequently demonstrated CRDT-based secure group communication in decentralized networks, reporting that careful algorithm selection and state compression strategies can mitigate performance penalties to acceptable levels for moderate-scale deployments.

7. Blockchain Integration for Trust and Identity Management

1. Trust Challenges in Decentralized Communication

The elimination of centralized servers removes the conventional trust anchor that authenticates peers, manages identities, and enforces access control in traditional communication systems. Without such an authority, decentralized systems face challenges of peer authentication, identity verification, resistance to impersonation attacks, and non-repudiation. Zhou, Wu, and Wang (2024) identified these trust establishment challenges as a critical barrier to secure decentralized communication at scale, motivating investigation of blockchain-based mechanisms as distributed trust infrastructure.

2. Blockchain-Based Identity and Authentication

Blockchain technology provides a distributed, immutable, and tamper-evident ledger enabling trust establishment without reliance on central authorities. Zhou et al. (2024) demonstrated that blockchain-based identity frameworks allow users to maintain cryptographic identities verifiable in a decentralized manner, reducing dependency on centralized identity providers while improving transparency and accountability. Singh, Kumar, and Tanwar (2024) further developed blockchain-based trust management frameworks for decentralized networks, demonstrating resistance to identity spoofing and Sybil attacks through cryptographic binding of identities to distributed ledger records. Gupta, Kumari, and Tanwar (2023) proposed blockchain-based security frameworks for decentralized

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

applications, showing that decentralized authentication can achieve security properties comparable to centralized identity providers while maintaining verifiability without trusted third parties.

3. Integrity Verification and Accountability

Beyond identity management, blockchain can provide tamper-evident logging of communication events by recording cryptographic hashes of messages or transactions on a distributed ledger. This approach enhances non-repudiation and accountability without exposing message content (Zhou et al., 2024). Researchers across multiple studies have confirmed, blockchain-based identification schemes offer increased transparency and autonomy, they come with scalability and latency challenges. Thus, instead of a real-time message transport a vast majority of research papers agree that blockchain can be selectively employed for identity validation, key management, and trust establishment. This is an integrated methodology that tries to ease the balance between decentralisation and practical or functional capabilities. (Kang, Kim, & Kim, 2022; Singh et al., 2024).

8. Cloud Computing as Adaptive Infrastructure

1. Complementary Role of Cloud in Decentralized Systems

Cloud computing has conventionally been associated with centralized service delivery, but contemporary research increasingly positions cloud infrastructure as a complementary, rather than contradictory, element of decentralized communication architectures. Xu, Li, and Chen (2024) argued that cloud platforms offer elasticity, geographic distribution, and on-demand resource provisioning that can strategically enhance decentralized system performance without compromising the fundamental P2P communication model. In this framing, cloud resources function as a managed safety net rather than as the primary communication medium.

2. Bootstrap and Discovery Services

One of the most clearly defined roles for cloud infrastructure in decentralized systems is the provision of initial bootstrap and discovery services. In fully decentralized deployments, newly joining peers must locate existing participants without access to centralized directories. Several studies propose cloud-hosted rendezvous services that facilitate initial peer discovery, after which communication transitions to direct P2P connections (Xu et al., 2024). This design constrains cloud involvement to a brief initialization phase, preserving decentralization during the majority of communication sessions. Nguyen, Kim, and Park (2023) evaluated cloud-assisted decentralized messaging platforms and confirmed that this hybrid bootstrap strategy achieves peer discovery latency competitive with fully centralized alternatives while substantially reducing persistent cloud dependency.

3. Relay Fallback and Cost Implications

The cloud infrastructure is used to facilitate peer discovery, monitoring, bootstrap services and adaptive fallback strategies but not necessarily as the principal communication medium . By providing scalable, on-demand resources cloud computing is particularly suited to decentralised communication infrastructures.

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

Alabi et al. (2020) highlighted that without managed relay resources, a significant proportion of users would be unable to establish P2P connections in practice. Bui, Cesana, and Brambilla (2024) examined decentralized messaging requirements in edge and fog computing environments, demonstrating that adaptive relay fallback can be efficiently implemented using distributed edge cloud resources proximate to end-users, minimizing relay-induced latency. Xu et al. (2024) quantified the cost implications of relay usage, finding that continuous relay reliance significantly increases operational expenditure while selective fallback, triggered only upon direct connection failure, reduces relay bandwidth consumption by 60–80% in typical network environments. Yadav, Singh, and Tripathi (2025) further demonstrated that scalable hybrid P2P architectures incorporating adaptive cloud fallback achieve superior cost-performance trade-offs compared to either purely centralized or purely decentralized designs.

9. Comparative Analysis of Existing Systems

A structured comparison of existing communication systems illuminates the practical trade-offs between architectural choices. Table 1 summarizes key characteristics of representative platforms across the centralized-decentralized spectrum.

Table 1: Comparative Analysis of Communication Architectures

WhatsApp/ Signal:	Telegram	Zoom/Discord	WebRTC-based P2P	CRDT-based Decentralized	Proposed Hybrid Models
Centralized routing	Cloud-centric	Fully centralized	Direct peer communication	Consistent group messaging	P2P-first
E2EE content	Prioritizes synchronization and accessibility	Optimized for media streaming	Strong privacy	No central coordinator	Blockchain identity
Significant metadata exposure	Limited E2EE by default	High reliability	NAT/firewall challenges	Memory overhead at scale	CRDT consistency
High reliability	Persistent metadata storage	Extensive metadata and content processing	Relay dependency in restrictive environments	Computational overhead at scale	Cloud adaptive fallback

Riegel, Weber, and Wehrle (2022) conducted a comprehensive comparative evaluation of decentralized messaging architectures, confirming that purely decentralized systems consistently underperform centralized platforms in usability and reliability metrics while offering superior privacy properties. Parker and Riva (2022) demonstrated that platforms prioritizing E2EE content protection continue to

International Journal of Science and Engineering Science Research
Volume 2 | Issue 2 | April-June 2026 | ISSN 3049-2793
Peer Reviewed (Referred Journal)
DOI: https://doi.org/10.63671/ijsesr.v2i2.121

expose substantial metadata to service infrastructure. These findings collectively support the literature's emerging advocacy for hybrid architectures that capture the privacy benefits of decentralization while leveraging selective infrastructure support to address reliability gaps.

10. Challenges and Research Gap

A few problems remain open, after substantial studies. Especially in the context of mobile and heterogeneous networks, most decentralised messaging systems have difficulty competing with centralised ones in terms of usability and performance.One active threat to privacy is leaking metadata through peer discovery and network-level interactions.

Furthermore, there is a scarcity of comprehensive frameworks that integrate cloud-assisted fallback, consistency control, peer-to-peer communication and decentralized trust in the context of a real-time system. Existing studies often only focus on the part rather than

complete architectural form. Such comprehensive comparative research on centralisation, decentralisation and hybrid systems remain scarce today.

Synthesis of the reviewed literature reveals several unresolved challenges that constrain the practical realization of secure, scalable decentralized communication systems:

Metadata Privacy: Current E2EE implementations protect message content but leave communication metadata broadly exposed. Integrated approaches combining content encryption with metadata minimization through decentralized routing remain underdeveloped.

NAT and Firewall Traversal: Reliable direct peer connectivity in restrictive network environments continues to require relay fallback infrastructure. Efficient, privacy-preserving NAT traversal without introducing centralized relay dependency is an open problem.

CRDT Scalability: CRDTs offer strong theoretical consistency guarantees but face practical overhead challenges in high-volume, large-scale group messaging. Optimized CRDT designs for mobile and resource-constrained environments are insufficiently explored.

Unified Framework Integration: Research goals should be focused on building integrated P2P-first architectures, with safe communication mechanisms, decentralised trust and efficient consistency mechanisms for adaptive infrastructure.The main goal of future research - Promising research avenues include intelligent relay avoidance techniques, optimised CRDT implementations for real-time messaging, and privacy-preserving peer finding.

Blockchain Latency: Blockchain technology has been studied for its application as a decentralised trust and identity management system. Skycoin advocates the ability for communities to have greater control over how information is stored, circulated and exchanged, and through decentralised data accountability routines, with no reliance on central authorities by employing a distributed immutable ledger that allows tamper-evident audit trails as well as cryptographic methods for identifying oneself.

Comparative Evaluation: System performance and resilience can be further improved by developments in distributed computing, secure identity management, and machine learning-assisted

DOI: https://doi.org/10.63671/ijsesr.v2i2.121

routing. To reduce the gap between conceptual research and practical adoption, large-scale investigational deployments and user-oriented consideration are crucial.

Usability and Adoption: Decentralized systems consistently report usability gaps relative to centralized alternatives. Human-centered design approaches that reconcile decentralization with user experience expectations represent an underexplored research dimension.

11. Conclusion

This review offers a structured evaluation of secure decentralised peer-to-peer communication systems, highlighting their potential to address the privacy, scalability, and resilience constraints of centralised architectures. This paper identifies hypercritical challenges and prospects for future systems by making whole research on WebRTC-based P2P communication, blockchain-enabled trust, CRDT-based consistency, and cloud-assisted adaptive fallback mechanisms.

The results indicate that blended architectures that prioritise decentralisation while selectively utilising cloud infrastructure provide a practical solution. The development of communication platforms that are scalable, privacy-preserving, and powerful in consistency with the changing needs of modern digital society demand ongoing research and cross-functional association.

References

1. Alabi, T., Naeem, M., Al-Rakhami, M., & Shin, K. G. (2020). Secure and scalable peer-to-peer communication in constrained network environments. IEEE Communications Surveys & Tutorials, 22(4), 2561–2585.
2. Alonso, R., Kossmann, D., & Wiesmann, M. (2021). Distributed systems consistency models revisited. ACM Computing Surveys, 53(4), 1–37.
3. Anderson, R., Berg, S., & Feamster, J. (2022). Metadata privacy in modern messaging systems. IEEE Security & Privacy, 20(3), 28–36.
4. Baquero, C., & Moura, F. (2020). Conflict-free replicated data types for real-time collaborative systems. Journal of Parallel and Distributed Computing, 145, 1–14.
5. Bano, S., Al-Bassam, M., & Danezis, G. (2021). Communication without servers: A survey of decentralized messaging systems. ACM Computing Surveys, 54(6), 1–38.
6. Bui, N., Cesana, M., & Brambilla, S. (2024). Decentralized messaging for edge and fog computing environments. Future Internet, 16(2), 61.
7. Cao, Y., Li, X., & Wang, P. (2024). Adaptive relay avoidance in peer-to-peer networks. Computer Networks, 244, 110245.
8. Das, S., Majumdar, A., & Sen, S. (2023). Peer-to-peer overlays for scalable real-time applications. Journal of Systems Architecture, 139, 102885.
9. Frosch, T., Mainka, C., Bader, C., Bergsma, F., Schwenk, J., & Holz, T. (2021). How secure is end-to-end encryption? IEEE Security & Privacy, 19(4), 28–39.
10. Gupta, R., Kumari, A., & Tanwar, S. (2023). Blockchain-based security frameworks for decentralized applications. Future Generation Computer Systems, 140, 367–381.
11. Haque, M., Islam, S., & Rahman, T. (2022). Performance analysis of peer-to-peer messaging over WebRTC. International Journal of Computer Networks & Communications, 14(3), 1–17.
12. Jennings, C., Johnston, A., & Jensen, M. B. (2021). WebRTC: Real-time communication for the web. IEEE Internet Computing, 25(3), 72–79.

13. Kang, J., Kim, Y., & Kim, D. (2022). Decentralized identity and authentication for P2P communication. Computer Standards & Interfaces, 82, 103620.
14. Mahmoud, H. (2025). A systematic review on WebRTC for potential applications and challenges. Multimedia Tools and Applications, 84(4), 6021–6050.
15. Nguyen, G. T., Kim, K., & Park, Y. (2023). Cloud-assisted decentralized messaging platforms. Journal of Cloud Computing, 12(1), 45–60.
16. Parker, S., & Riva, F. (2022). Metadata leakage in encrypted messaging systems. ACM Computing Surveys, 55(2), 1–36.
17. Pietzuch, P., Shneidman, J., & Roussopoulos, M. (2020). Consistency trade-offs in distributed messaging systems. IEEE Distributed Systems Online, 21(2), 23–31.
18. Rahman, M., Hasan, K., & Rahman, M. (2024). Latency optimization techniques for P2P communication. Computer Communications, 214, 112–123.
19. Riegel, M., Weber, J., & Wehrle, K. (2022). Decentralized messaging systems: Architectures, security and performance. Computer Networks, 207, 108873.
20. Shapiro, M., Preguica, N., Baquero, C., & Zawirski, M. (2022). Conflict-free replicated data types. Communications of the ACM, 65(3), 90–99.
21. Singh, A., Kumar, R., & Tanwar, S. (2024). Trust management in decentralized networks using blockchain. IEEE Access, 12, 34112–34125.
22. Wang, H., Sun, Y., & Zhou, X. (2022). Real-time communication over WebSockets: Limitations and enhancements. IEEE Internet Computing, 26(6), 56–64.
23. Xu, H., Wang, T., & Liu, J. (2024). Adaptive relay selection for peer-to-peer communication systems. Computer Communications, 213, 89–101.
24. Xu, Y., Chen, L., & Wang, H. (2023). Performance evaluation of WebSocket and HTTP/2 based real-time messaging systems. Journal of Network and Computer Applications, 210, 103518.
25. Xu, Y., Li, Z., & Chen, M. (2024). Cloud-assisted decentralized communication architectures for resilient messaging systems. Future Generation Computer Systems, 151, 321–335.
26. Yadav, R., Singh, P., & Tripathi, A. K. (2025). Scalable decentralized messaging using hybrid P2P architectures. Future Generation Computer Systems, 152, 98–110.
27. Zhang, Q., Li, J., & Ren, K. (2021). Communication protocol evolution for real-time systems. IEEE Transactions on Network and Service Management, 18(4), 4127–4141.
28. Zhang, R., Hu, Y., & Chen, Q. (2024). Secure group communication using CRDTs in decentralized networks. IEEE Transactions on Dependable and Secure Computing, 21(2), 811–824.
29. Zhang, Y., Wang, H., & Chen, L. (2023). Secure peer discovery mechanisms in decentralized networks. IEEE Access, 11, 88231–88244.
30. Zhou, L., Wu, Y., & Wang, X. (2024). Blockchain-based decentralized identity management. IEEE Transactions on Information Forensics and Security, 19, 1023–1037.
31. Zhou, L., Sun, H., & Zhang, Y. (2025). Peer-to-peer network design for scalable communication systems. Computer Communications, 215, 45–58.