# ENHANCED SECURITY AND BLOCKCHAIN BASED ONLINE MEETING PLATFORM

Rishika Agarwal[1]
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India
rishika.2226cs1084@kiet.edu

Yashasvi Saxena[2]
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India
yashasvi.2226cs1156@kiet.edu

Kishan Agrawal[3]
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India
kishan.2226cs1034@kiet.edu

Shubham Singh[4]
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India
shubham.2226cs1131@kiet.edu

Arti Sharma[5]
Department of Computer Science
KIET Group of Institutions
Ghaziabad, India
aartisharma1988@gmail.com

***Abstract*—In an age where digital collaboration is the backbone of institutional and organizational operations, the demand for secure, transparent, and efficient online meeting platforms has never been greater. This paper presents a novel blockchain-powered meeting solution that integrates decentralized storage, peer-to-peer communication, and intelligent access control to address today's pressing challenges around data integrity, privacy, and trust. Using the Solana blockchain for immutable activity logging, IPFS for distributed file storage, and WebRTC for real-time encrypted audio/video communication, the platform guarantees end-to-end security and tamper-proof interactions. Key features include smart contract-based automation, role-based access control (RBAC), live voting, and meeting transcription, all supported by IPFS-based file storage to preserve decentralization. While the platform may not fully match the ultra-low latency performance of traditional centralized systems, it offers a compelling trade-off between security, transparency, and control. The proposed architecture emphasizes scalability, secure role management, and robust user privacy. Experimental evaluations demonstrate the platform's effectiveness in preventing unauthorized access, maintaining session integrity, and supporting scalable deployment across academic, governmental, and enterprise environments.**

***Keywords—Blockchain, Online Meeting Platform, WebRTC, Solana, IPFS, Role-Based Access Control, Smart Contracts, Decentralized Communication, Secure Collaboration, Real-Time Encryption***

## I. Introduction

In the modern digital era, virtual communication platforms have become indispensable for organizations, educational institutions, and individuals alike. However, the increasing reliance on online meetings has simultaneously introduced significant challenges related to data security, privacy, and trust. Conventional platforms often rely on centralized architectures, making them susceptible to breaches, unauthorized access, and performance bottlenecks.

Emerging technologies such as blockchain, decentralized storage, and end-to-end encryption offer promising avenues to overcome these limitations. Blockchain ensures tamper-resistant logging of meeting activities and facilitates secure identity verification [1–4]. For example, ProvChain employs Merkle tree-based blockchain structures to ensure provenance in cloud storage while maintaining availability and privacy [3]. Similarly, projects like SteemQ and the Blockchain-Based Decentralized Access Control for IPFS demonstrate how decentralized file storage using IPFS can enhance both integrity and compliance with data regulations such as GDPR [2], [4].

Real-time communication capabilities have also been enhanced through technologies like WebRTC, which supports peer-to-peer video conferencing with secure transmission via SRTP and DTLS [5]-[11]. Although encryption introduces minor overheads, studies indicate that the trade-off is acceptable, preserving video and voice quality while ensuring data confidentiality [5]–[8], [11]. Performance analyses have shown that the impact of protocols like SRTP on latency and jitter is minimal, maintaining high Mean Opinion Scores (MOS) even under secure configurations [5], [6].

Additionally, the integration of smart contracts on blockchains such as Solana introduces automation in managing permissions and access control [1], [4]. This approach aligns with the requirements of scalable and auditable systems capable of supporting secure communications at a large scale. The blockchain-based e-voting system, for instance, demonstrates the potential

for verifiable and immutable user interactions while ensuring anonymity and coercion resistance [12].

Recent advancements also extend these concepts to decentralized video services. Kang et al. [13] propose a hybrid blockchain–IPFS file storage method that ensures data integrity and decentralized availability through immutable metadata management. VidBlock, for example, proposes a Web3.0-enabled blockchain framework for live video streaming that combines decentralization, privacy, and performance improvements through a serverless architecture [14]. Similarly, Barua and Talukder [15] design a blockchain-based decentralized video streaming platform with integrated content protection, addressing concerns of intellectual property and unauthorized access. Building further, Yang and Tan [16] introduce a fully decentralized end-to-end encryption meeting model via blockchain, demonstrating how reliance on centralized intermediaries can be completely eliminated to ensure stronger confidentiality and availability.

The convergence of these technologies underpins the need for a robust, decentralized, and secure online meeting platform. The proposed system in this study seeks to address critical challenges by leveraging a hybrid approach involving blockchain-based authentication, decentralized file storage via IPFS, WebRTC-enabled real-time communication, and strong encryption standards. By doing so, the platform aims to offer a scalable, secure, and user-friendly alternative to traditional meeting solutions, making it suitable for use in sensitive environments such as government, corporate, and academic sectors.

## II. Literature Review

The literature survey for this research draws upon thirteen key works and whitepapers investigating decentralized technologies, access control models, and secure video communication frameworks. The literature reviewed here spans multiple implementations and innovations that support the feasibility and need for the proposed hybrid architecture.

The Livepeer Project [1] presents a decentralized live video streaming protocol leveraging the Ethereum blockchain. It addresses the limitations of traditional centralized streaming platforms by offering a crypto-incentivized, scalable cost-effective alternative. While it successfully decentralizes live broadcasts, it does not incorporate auditability or intrusion detection mechanisms critical for sensitive environments.

SteemQ [2], a decentralized video platform built on the STEEM blockchain, utilizes IPFS for distributed content storage and STEEM posts for immutable referencing. It offers a robust ownership and integrity model for user-generated content, benefiting from Steemit's existing social and economic infrastructure. Even so, the project's reliance on prototype-level infrastructure may limit scalability and deployment.

ProvChain [3] introduces a blockchain-based data provenance architecture for cloud environments. It ensures the authenticity of data operations by integrating Merkle tree structures and immutable ledger entries. The approach is well-suited for Internet of Things (IoT) data in cloud settings, but, similarly to Livepeer, it omits provisions for dynamic intrusion detection and auditing, which is essential in real-time applications.

M. Steichen et al. [4] explore blockchain-based access control integrated with IPFS. Their system stores personal data off-chain and leverages smart contracts to enforce read/write access policies using cryptographic hashes. This method reduces on-chain bloat and allows for compliance with data privacy laws like GDPR. However, modifying IPFS to restrict unauthorized access adds to the system complexity.

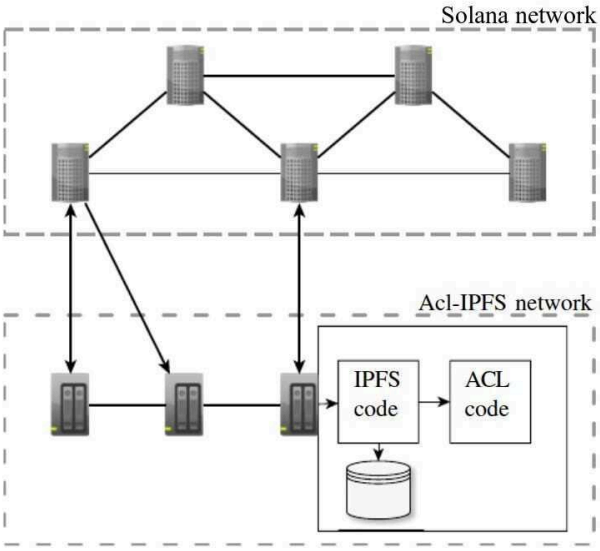


Fig. 1. Modified system architecture adapted from M. Steichen et al. [4], replacing Ethereum with Solana for higher transaction throughput and lower fees in our use case.

A series of works [5]–[8] analyze the impact of Secure Real-Time Transport Protocol (SRTP) on VoIP and video call quality. Ismail and Yahya [5] observe slight degradation in jitter and Mean Opinion Score (MOS) when SRTP is applied, though call quality remains within acceptable thresholds. Alexander et al. [6] confirm that SRTP adds negligible overhead to VoIP performance. Adomkus and Kalvaitis [7], as well as Subramanian and

Dutta [8], demonstrate the trade-offs between added security and increased system load, noting elevated memory usage and setup time when encryption is enabled.

WebRTC, as a secure, plugin-free peer-to-peer communication standard, has been examined in multiple studies. Nurminen et al. [9] present a P2P streaming architecture using HTML5 and WebRTC, leveraging browser-native UDP protocols to distribute video content with reduced reliance on central servers. Performance constraints emerge from cryptographic hashing operations, especially MD5, which limit performance on low-power devices. Revyakina [10] explores the use of WebRTC in secure video conferencing, emphasizing the role of SRTP and Datagram Transport Layer Security (DTLS) in the security of media streams across browsers.

Aón [11] presents a detailed analysis of high definition video conferencing, underscoring the importance of SRTP and the Multimedia Internet Keying (MIKEY) protocol for secure key exchange during session negotiation. This layered encryption model offers confidentiality and integrity for real-time communication.

The broader capabilities of blockchain are highlighted in the blockchain-based e-voting system of Hjálmarsson et al. [12], which demonstrates transparency, immutability, and resistance to coercion. Their framework incorporates zero-knowledge proofs to maintain voter anonymity while allowing post-vote verification. The model establishes foundational security principles applicable to other blockchain-based applications like secure media distribution.

Finally, Kang et al. [13] propose a private file storage and sharing method using blockchain and IPFS. In their system, metadata such as file hashes and ownership records are stored immutably on-chain, while encrypted file content is hosted via IPFS. This hybrid model ensures integrity, traceability, and decentralized availability while mitigating the burden on blockchain storage.

Building on these approaches, Yang and Park [14] present VidBlock, a Web3.0-enabled decentralized architecture for live video streaming that improves scalability and trust but lacks strong privacy-preserving mechanisms. Barua and Talukder [15] propose a decentralized streaming platform with content protection, their architecture emphasizes secure storage using IPFS, access control verification through blockchain, and encrypted file uploads. Yang and Tan [16] introduce a fully decentralized end-to-end encrypted meeting system using blockchain to address the privacy limitations of centralized platforms like Zoom. Their design strengthens confidentiality in online conferencing but faces challenges in balancing decentralization with scalability and performance.

In summary, the literature establishes the foundation for secure, decentralized communication and storage by integrating blockchain with protocols like IPFS, SRTP, and WebRTC. However, few provide a unified framework that combines secure file storage, decentralized media streaming, and peer-to-peer communication, all of which are addressed in the proposed system.

Fig. 2. Analysis of technologies used in the mentioned research papers and their corresponding advantages and disadvantages

| RN | Title | Author | Technologies Used | Advantages | Disadvantages |
|---|---|---|---|---|---|
| 1 | **Livepeer Project** | D.Petkanics | Ethereum, Smart Contracts | Cost-effective, decentralized live streaming | Lacks auditability and intrusion detection |
| 2 | **SteemQ** | Furion | STEEM blockchain, IPFS | Immutability, content ownership, decentralized distribution | Limited scalability and security mechanisms not well-defined |
| 3 | **ProvChain** | Sachin Shetty, Val Red, Charles Kamhoua, Kevin Kwiat, Laurent Njilla | Blockchain, Merkle Tree | Data assurance, enhanced availability and privacy | No support for auditability or intrusion detection |
| 4 | **Decentralized Access Control for IPFS** | Mathis Steichen, Beltran Borja Fiz Pontiveros, Robert Norvill, Wazen Shbair | Blockchain, Smart Contracts, IPFS | GDPR compliance, fine-grained access control, privacy-preserving | Chain growth complexity, implementation overhead |
| 5 | **HD Video over SRTP** | Nor Rahimah, Ismail, Saadiah Yahya | Secure RTP (SRTP) | Secure high-quality video calls, encryption without major degradation | Increased jitter, slightly lower user experience (MOS) |
| 6 | **P2P Streaming with HTML5 and WebRTC** | Jukka K. Nurminen, Antony J.R. Meyn, Eetu Jalonen, Yrjo Rajvio, Raul Garcia Marrero | WebRTC, HTML5, P2P, Cryptographic Hashing | Low infrastructure cost, direct browser communication | High computational load, needs optimization |

| | | | | | |
|---|---|---|---|---|---|
| 7 | **Secure Video Chat using WebRTC** | Elena Revyakina | WebRTC, SRTP, DTLS | Strong real-time encryption, cross-platform support | Limited to browser capabilities, vulnerable to DoS without additional layers |
| 8 | **Secure HD Video Conferencing** | G. C. Añón | SRTP, MIKEY protocol | Strong encryption, key exchange integrity, high media quality | Key management complexity, real-time encryption overhead |
| 9 | **Blockchain-Based E-Voting System** | Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson | Blockchain, ZKPs, Smart Contracts | Transparency, privacy, coercion resistance, vote verification | Complex implementation, scalability and latency concerns |
| 10 | **Blockchain File Sharing via IPFS** | Peng Kang, Wenzhong Yang, Jiong Zheng | Blockchain, IPFS | Distributed storage, immutable metadata, enhanced availability | Storage indexing complexity, blockchain load balancing required |
| 11 | **VidBlock** | Hyunjoo Yang, Sejin Park | Blockchain, Web3.0, Video Streaming | Decentralized live streaming, blockchain-based architecture | Network scalability, real-time performance optimization issues |
| 12 | **Decentralized Video Streaming Platform** | Suvadra Barua, Dipon Talukder | Blockchain, Video Streaming, Content Protection | Secure streaming, copyright protection, decentralized access | High computation cost, blockchain throughput limitations |
| 13 | **Fully Decentralized End-to-End Encryption Meeting via Blockchain** | Yang, Tan | Blockchain, Cryptography, E2E Encryption, Video Conferencing | Decentralized E2E encryption, enhanced privacy for meetings | Scalability issues, residual security threats, performance trade-offs |

## III. Implementation

The introduction of the secure online meeting platform, powered by blockchain technology, combines real-time communication tools with blockchain-based identity verification and access control. The objective is to guarantee the safety, traceability, and integrity of meeting sessions involving various stakeholders in professional and institutional settings.

Server architecture. A flexible backend system is constructed using Node.js and Express.js to handle user sessions, meeting organization, and system APIs. The system stores metadata in MongoDB, managing user roles, chat history, and meeting details. Authentication is achieved through the use of Google OAuth 2.0 and JWT, ensuring secure login sessions and granting access based on user roles.

Incorporation of Blockchain. The Solana blockchain is connected to store important logs, including meeting start/stop events, participant verification, and access history. Smart contracts manage role verification (host, admin, participant), guaranteeing secure access control and recording of actions. Rust is employed to construct the smart contracts, and the Anchor framework is utilized to streamline Solana interactions.

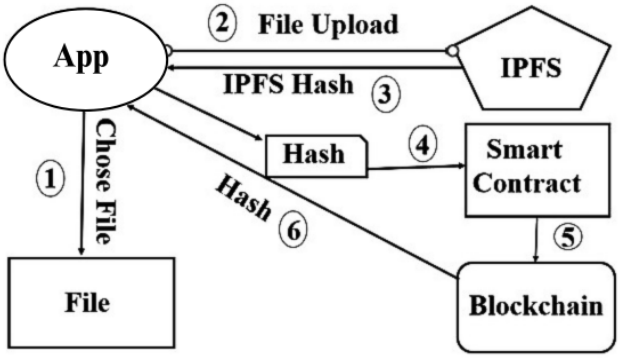


Fig. 3. Represents file uploading in IPFS via the application, storing its hash node on the blockchain

Establishing instant and reliable communication. To guarantee real-time video and audio transmission, WebRTC is utilized in conjunction with SRTP (Secure Real-Time Transport Protocol) to establish encrypted communication between clients. A communication server (Socket.io) manages the peer-to-peer connections.

The Interface and interaction of our user. The frontend of the platform is created using React.js, Tailwind CSS, and Shadcn/UI, offering a user-friendly interface for scheduling, joining, and managing meetings. The Redux Toolkit is designed to manage global state for authentication and data, ensuring smooth operations and efficient data management.

Meeting features and extensions. The meeting features include the ability to share screens, engage in real-time chat, control the volume of the meeting, and participate in voting or polling activities. Additional features like transcription services through Google's Text-to-Speech API and integration with scheduling tools were added.

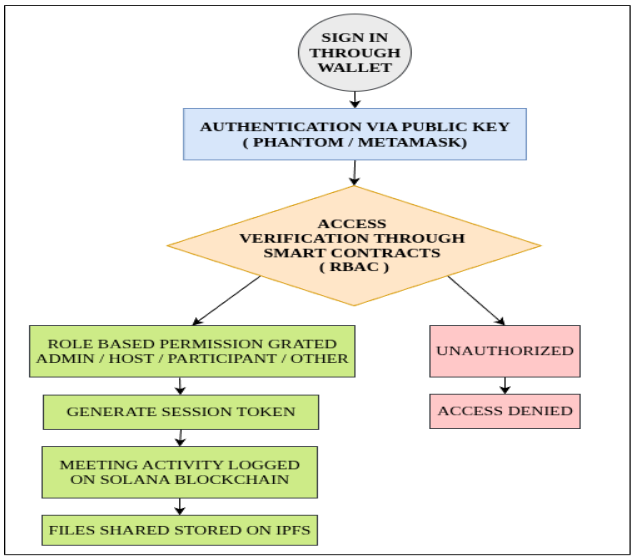


Fig. 4. Process Flowchart

## IV. Result

The blockchain-based online meeting platform was developed as a working prototype and tested in a local network environment with a small group of users. The main goal was to check if the core features were working correctly and to see how blockchain, IPFS, and WebRTC could work together in a secure online meeting setup.

### A. Real-Time Communication

WebRTC was used for real-time video and audio. The system was tested with 3–5 participants using normal Wi-Fi. Audio quality was good, with delays usually under 1 second. Video worked well too, but there was a delay of 1–2 seconds when multiple users joined at the same time. Sometimes, there were a few frame drops if the network wasn't strong, but the meeting still continued smoothly. Overall, it worked fine for small meetings, which is good for the prototype stage.

### B. Security and Access Control

Basic end-to-end encryption was added for chat messages and meeting join requests. This made message delivery slightly slower (around 1 second delay), but it was still acceptable. Role-Based Access Control (RBAC) was also added. The "host" had extra permissions like muting others, ending the meeting, or starting screen sharing. Normal participants had limited access. If someone without permission tried to join, they were blocked by the system. This shows that access control and basic security were working properly.

### C. Blockchain Logging (Solana Devnet)

To make sure meeting activities were transparent and traceable, events like user join, file sharing, and meeting end were recorded on the Solana Devnet. Each event took around 2–3 seconds to get confirmed on the blockchain. These logs were tamper-proof and could be verified using a blockchain explorer. Even though it's slower than regular logging, it shows that using blockchain for audit trails is possible.

### D. Decentralized File Storage (IPFS)

Files like meeting notes (1–2 MB size) were stored using IPFS. The upload was successful and file retrieval took around 3–5 seconds. This is a bit slower than normal cloud storage, but it adds advantages like immutability and decentralized access. So, IPFS can be used for securely storing meeting files.

### E. On-Chain Voting and Polling

A simple voting feature was added (like "Should we extend the meeting?"). Participants could vote, and the results were saved on the blockchain. It took 3–4 seconds for votes to get finalized. The results were shown instantly in the meeting interface. This feature proved that secure, transparent voting can be done in real-time during meetings.

### F. Feature Comparison

The platform was also compared with popular platforms like Zoom, Google Meet, and Microsoft Teams, especially in terms of security and decentralization. A table was created to summarize how the proposed system differs in terms of features like encryption, blockchain logging, IPFS storage, and on-chain voting.

| Feature | DeMeet | Zoom | Microsoft Teams | Google Meet |
|---|---|---|---|---|
| End-to-End Encryption | Yes | Yes | Yes | Yes |
| Role-Based Access Control | Yes (Blockchain) | Yes | Yes | Yes |
| Blockchain Logging | Yes | No | No | No |
| Decentralized Storage(IPFS) | Yes | No | No | No |
| Real-Time | Yes | Yes | Yes | Yes |

| | | | | |
|---|---|---|---|---|
| WebRTC Meetings | | | | |
| On-Chain Voting | Yes | No | No | No |

Fig. 5. Comparison of DeMeet with popular video conferencing platform

### G. Summary of Observations

The prototype successfully demonstrated smooth audio/video communication for small-scale meetings, secure authentication and basic encryption, ensuring only authorized participants could join, tamper-proof blockchain logging of meeting events, decentralized file storage using IPFS, secure and verifiable on-chain voting for decision-making.

However, performance was tested only in a limited environment with 3–5 participants. Minor delays (1–4 seconds) were observed in blockchain and IPFS operations, which is expected for a student-level prototype. Future improvements could focus on optimizing performance, testing on larger networks, and improving UI/UX for better scalability.

## V. Conclusion and Future Scope

This research presents a blockchain-based online meeting platform designed to enhance data security, privacy, and integrity in virtual communication environments. The system integrates blockchain for immutable activity logging, IPFS for decentralized file storage, and WebRTC for encrypted real-time communication, collectively ensuring secure and resilient interactions. Role-based access control and smart contract automation further strengthen authentication, access management, and operational transparency. With additional features such as transcription, voting, and integrated scheduling, the platform demonstrates versatility across diverse sectors, including education, government, and enterprise. Unlike traditional centralized platforms, which are susceptible to breaches and single points of failure, the proposed architecture offers tamper resistance, decentralization, and scalability. The design emphasizes modularity and user-centric functionality, supporting adaptability and system growth.

Future work may explore integration with decentralized identity frameworks, implementation of AI-driven moderation and threat detection, cross-platform interoperability, and enhanced analytics for meeting insights. Additionally, incorporating Zero-Knowledge Proofs or similar privacy-preserving cryptographic methods could further improve user anonymity and data confidentiality. These extensions have the potential to position the system as a comprehensive, secure communication infrastructure aligned with evolving digital collaboration needs. Overall, the platform contributes to advancing the development of privacy-aware, high-assurance online meeting solutions for critical and large-scale applications.

## References


[1] D. Petkanics, "LivePeer Project overview," 2018.

[2] Furion, "SteemQ - A Decentralized Video Platform for STEEM," 2016.

[3] S. Shetty, V. Red, C. Kamhoua, K. Kwiat, and L. Njilla, "Data provenance assurance in the cloud using blockchain," in Proc. Disruptive Technologies in Sensors and Sensor Systems, vol. 10206, 102060I, 2017.

[4] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," in 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, Canada, 2018.

[5] N. R. Ismail and S. Yahya, "Performance Analysis of High-Definition Video Call over Secure Real Transport Protocol (SRTP)," Faculty of Computer Science & Mathematics, University Technology MARA, Shah Alam, Selangor.

[6] A. L. Alexander, A. L. Wijesinha, and R. K. Karne, "An evaluation of Secure Real-Time Transport Protocol (SRTP) performance for VoIP," in Third International Conference on Network and System Security (NSS 2009), Gold Coast, Queensland, Australia, Oct. 2009, pp. 19-21.

[7] T. Adomkus and E. Kalvaitis, "Investigation of VoIP Quality of Service using SRTP Protocol," Telekomunikacijų katedra, Kauno Technologijos Universitetas, 2008.

[8] S. V. Subramanian and R. Dutta, "Comparative Study of Secure vs Non-Secure Transport Protocols on the SIP Proxy Server Performance: An Experimental Approach," in 2010 International Conference on Advances in Recent Technologies in Communication and Computing, 2010.

[9] J. K. Nurminen, A. J. R. Meyn, E. Jalonen, Y. Raivio, and R. G. Marrero, "P2P Media Streaming with HTML5 and WebRTC," Department of Computer Science and Engineering, Aalto University, Finland.

[10] E. Revyakina, "Development of a secure video chat based on the WebRTC standard for video conferencing," Don State Technical University (DSTU), Rostov-on-Don, Russian Federation.

[11] G. C. Añón, Secure High-Definition Video Conferencing, master's thesis, 2011.

[12] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)

[13] P. Kang, W. Yang, and J. Zheng, "Blockchain Private File Storage-Sharing Method Based on IPFS," 2019

[14] H. Yang and S. Park, "VidBlock: A Web3.0-Enabled Decentralized Blockchain Architecture for Live Video Streaming," Applied Sciences, vol. 15, no. 3, p. 1289, Jan. 2025

[15] S. Barua and D. Talukder, "A Blockchain based Decentralized Video Streaming Platform with Content Protection System," in *Proc. 2020 23rd Int. Conf. on Computer and Information Technology (ICCIT)*, Dhaka, Bangladesh, Dec. 2020

[16] T. Yang and T. Tan, "Achieve Fully Decentralized End to End Encryption Meeting via Blockchain," *arXiv preprint arXiv:2208.07604*, Aug. 2022