International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 15, No. 3, September 2026, pp. 1313~1321
ISSN: 2252-8776, DOI: 10.11591/ijict.v15i3.pp1313-1321

An effective blockchain-based system for tracking viral content origins in social media

Nageswararao Sirisala[1], Srinivasulu Sirisala[2], Nalavala Ramanjaneya Reddy[3], Syed Anisha[1]
[1]Department of Computer Science and Engineering, K.S.R.M. College of Engineering, Kadapa, India
[2]Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, India
[3]Department of Computer Science and Engineering, R.G.M. College of Engineering and Technology, Nandyal, India

Article Info

Article history:

Received Jun 27, 2025
Revised Apr 10, 2026
Accepted May 17, 2026

Keywords:

Blockchain
Cryptographic hashing
Decentralized storage
Digital rights management
Ethereum
Fake content detection
Interplanetary file system
Smart contracts
Web3

ABSTRACT

Tracking the origins of viral content in social media is crucial for identifying misinformation, ensuring accountability, and protecting intellectual property. By tracing content back to its source, platforms can curb the spread of false narratives, hold malicious actors responsible, and safeguard creators' rights. In this work, "Effective blockchain based system for tracking viral content origins in social media-(BCTVCO)" is proposed. The BCTVCO is a blockchain-based content authentication platform that leverages interplanetary file system (IPFS), smart contracts, and cryptographic hashing to verify digital assets and detect unauthorized reuse. This decentralized application addresses the challenges of content authenticity, ownership verification, and intellectual property protection in the digital space. The system integrates Ethereum smart contracts (Solidity) to store immutable content records and uses SHA-256 hashing for secure file integrity verification. Content is uploaded to IPFS via Web3. Storage, ensuring distributed and tamper-resistant storage. The React-based frontend with MetaMask authentication allows users to seamlessly register, upload, and track their content. In implementation, BCTVCO outperformed existing methods and proved to be a scalable, transparent, and secure blockchain-based content verification system. Future enhancements of BCTVCO involve multi-chain support and AI-powered content analysis to strengthen security and usability.

Corresponding Author:

Srinivasulu Sirisala
Department of Computer Science and Engineering, CVR College of Engineering
Hyderabad, Telangana, India
Email: vasusirisala@gmail.com

1. INTRODUCTION

The rapid proliferation of viral content on social media platforms has revolutionized the way information spreads, both favourably and negatively. The quick spread of viral content on social media platforms has completely changed how information is disseminated. Viral material has the power to change attitudes, create trends, and even affect societal consequences on social media sites like Facebook, Instagram, TikTok, and Twitter, which are accessed by billions of users. Finding the source of viral content, monitoring its spread, and confirming its legitimacy are some of the difficulties it presents. Misinformation and disinformation are frequently propagated as a result of a lack of openness surrounding the production and dissemination of content. By providing a decentralized, impenetrable system that makes it possible to monitor the sources of viral information in a transparent and safe way, blockchain technology offers a potential remedy for these problems. A system that documents the production and spread of viral content on

social media platforms and offers a transparent record of its beginnings and changes over time can be created by utilizing the distributed and immutable characteristics of blockchain technology. The Blockchain-Based System for Tracking the Origins of Viral Content in social media (BCTVCO) is presented in this study. Blockchain technology is used by the system to guarantee viral content traceability, accountability, and transparency. This technology makes it possible to identify the content's original source and track changes, shares, and reposts in real time.

Here are several effective methods will track the origins of viral content in social media.

- Digital watermarking: even if media information is altered or shared again, platforms and authorities can still identify the original source by embedding visible or invisible tags in it.
- Reverse image and video search: Tin Eye and Google reverse image search are two tools that can determine when visual content first appeared online.
- Blockchain technology: blockchain ensures unambiguous traceability and authenticity by providing a tamper-proof ledger that records the generation of material.
- Network analysis: researchers can determine the original source and important influencers by examining the ways that content spreads throughout social media sites.
- URL tracking: UTMs, or unique URL parameters, aid in tracking the origin of shared material.
- Machine learning and AI tools: Viral material can be efficiently traced by AI algorithms taught to recognize sentiment analysis, contextual cues, and content dissemination patterns.

The proposed BCTVCO system offers key advantages for secure and reliable content tracking. The system enhances accountability by linking content to its creators and distributors, and decentralization eliminates reliance on a single authority. Additionally, cross-platform compatibility supports monitoring across different social media networks, improving content moderation and reducing the spread of misinformation.

2. LITERATURE SURVEY

Blockchain technology has become a potent instrument for guaranteeing the provenance, authentication, and security of digital content in a variety of fields. A blockchain-based method for tracking digital content using cryptographic hashes, guaranteeing content integrity and preventing tampering, is suggested [1]. Shu *et al.* [2], an integrated method in fake news detection is proposed, where AI models were paired with blockchain to confirm news authenticity. This increased confidence but needed broad adoption to be effective. Zyskind *et al.* [3] present a self-sovereign identity (SSI) system that uses blockchain to authenticate users, improving security and privacy but requiring better usability for widespread adoption. A blockchain-based social media platforms like Steemit are examined, showing that decentralized media is feasible but also pointing out the dangers of token value volatility [4].

Verification of digital content is another important use case for blockchain technology. Cryptographic signatures were introduced by the Adobe Content Authenticity Initiative to confirm media authorship; their efficacy depends on content providers' collaboration [5]. Blockchain technology was used for picture verification [6], which increased digital image trust but required interaction with well-known systems. A blockchain-based authentication system for journalism is proposed that improved public trust in the field but had latency problems when disseminating news in real time [7], [8]. Reddy *et al.* [9] an enterprise-level hierarchical model with a secure data protocol was introduced, emphasizing secure data transmission and integrity across distributed applications. The difficulties and potential paths of AI-powered false content identification were emphasized [10]-[12], and the necessity of big datasets to increase accuracy. For decentralized content authentication, IPFS is combined with machine learning to improve security but necessitates optimization for practical use [13], [14]. Additionally, an AI-enabled blockchain system for content ownership verification and fraudulent content identification was created in [15], which greatly increased accuracy but required scalability improvements.

A smart contract-based method for digital media copyright enforcement was presented in [16]; it offers automated enforcement but has trouble getting legal adoption. A blockchain-based copyright protection strategy was presented in [17], [18], which improved enforcement capabilities but necessitated wider legal recognition. In a similar way in [19], how smart contracts can safeguard digital assets is investigated, enhancing ownership transparency but requiring more robust legal support. Sangeeta and Nam [20] created a content-addressed, peer-to-peer storage system to improve data availability, but it has problems with network congestion. Blockchain was used to handle data in a way that protects privacy, improving user control while posing security issues during deployment in [21]. Ethereum's decentralized framework is proposed, which offers self-executing smart contracts but has problems with excessive energy consumption [22], [23].

3. PROPOSED METHOD (BCTVCO)

By utilizing blockchain technology, BCTVCO improves accountability and transparency. The blockchain stores a cryptographic hash, which acts as a unique identification. The content hash, information, and interactions like sharing and editing are all recorded by smart contracts. These contracts, which are written in Solidity and deployed through the Remix IDE, automate transaction logging and verification. A proof of stake (PoS) technique is used by the system for effective and decentralized validation. Blockchain transactions connected to the original hash are used to track the spread of content. Administrators and auditors are able to identify false information and track down the source of content. Smart contracts ensure tamper-proof execution by automatically reviewing or removing flagged content if it exceeds a fake-count threshold. While auditors track the impact of submissions, creators keep an eye on their status. By restricting changes or deletions, BCTVCO guarantees an unchangeable content history. This ensures the integrity of the content, fights false information, and encourages responsibility in the distribution of digital content. The methodology involves three major steps:

- Content identification and registration: using cryptographic techniques, content is given a unique identification, like a content hash, when it is produced or shared on a social media network. The blockchain then records this hash.
- Monitoring and recording transactions: a new transaction including the specifics of the exchange (such as the timestamp, user information, and platform information) is generated each time the item is shared, reposted, or altered.
- Verification and uditing: to confirm the content's provenance and history, users and platform moderators can send queries to the blockchain. Because the blockchain is decentralized, all records are available to the public and the data is protected against tampering for audit.

3.1. Architecture of BCTVCO system

Figure 1 illustrates the architecture of the BCTVCO system, where users interact through social media platforms integrated with blockchain layers. The blockchain infrastructure supports several core components, including nodes/validators, the content tracking system, and smart contracts to ensure transparency and data integrity. Furthermore, the system enables tracking of original content sources, propagation history, and viral content dissemination, while providing analytical insights through the analytics dashboard.

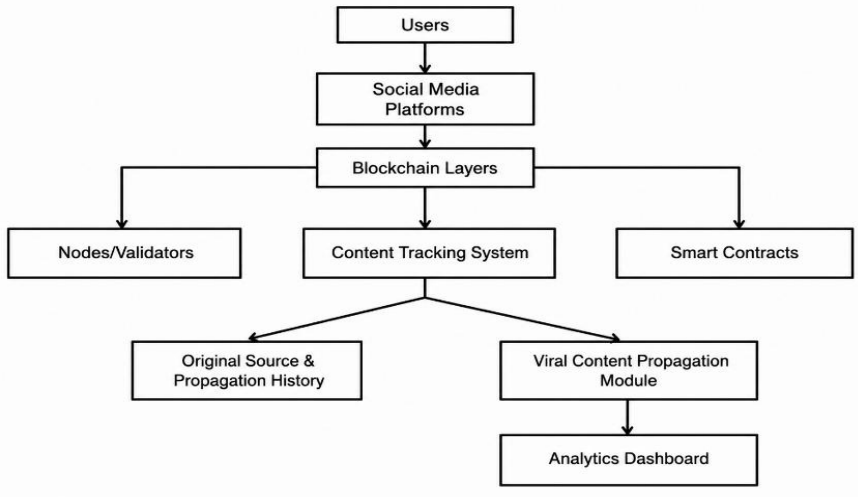

Figure 1. Flow of content from its creation to its tracking via the blockchain

3.2. Tracking out viral content origin

- Content hashing: each content item is maintained with a unique cryptographic hash (digital fingerprint), any minor changes to leads to produce a different hash, thus ensuring reliable content identification.
- Blockchain recording: a permanent and tamper-proof record will be created through a blockchain transaction that encompasses content hash, platform, timestamp, and user details.
- Propagation tracking: in connection with the original hash, every interaction (share/edit) is recorded as a new transaction, so that it forms a traceable chain that captures content spread and modifications across platforms.

- Blockchain querying: the complete history of a content, including origin, initial upload, and all subsequent interactions is maintained. This allows the users for real-time tracking.
- Immutable traceability: through the blockchain transactions, all interactions are recorded as resistant to manipulation.

3.3. Security threats and mitigations

Sybil attacks and mitigations. BCTVCO's reliance on crowd auditing and PoS validation creates potential for Sybil attacks-where an adversary generates many pseudo-identities to manipulate audits, flags, or validator elections [24], [25]. To mitigate this risk, a layered security approach is recommended: operating BCTVCO on a permissioned PoS or PBFT-style consortium with KYC-verified validators; requiring verifiable credentials (DID/SSI) for users involved in auditing; applying stake-backed weighted voting with slashing penalties for malicious behavior; and enabling rate-limiting alongside off-chain anomaly detection to identify fraudulent activity. Critical automated actions such as content removal should be protected using quorum or multi-signature approval, along with an appeal mechanism to avoid irreversible decisions triggered by Sybil-driven manipulation. Privacy concerns related to KYC can be addressed using selective disclosure and zero-knowledge proofs, ensuring Sybil-resistance while preserving user privacy [26].

4. RESULTS AND DISCUSSION

In this section, we outline the tools, algorithms, and technologies used in the implementation of BCTVCO.

Experimental setup*:* for effective and secure transaction validation, the BCTVCO system uses a PoS consensus process. Before moving to a public network, the blockchain architecture is developed on a local Hardhat node, which facilitates testing and the deployment of smart contracts. Content creation, sharing, verification, and auditing are managed by smart contracts created with Solidity in the Remix IDE. React.js, which was selected for the frontend due to its modularity and effective state management, allows for a responsive user interface for content audits. MetaMask is used to achieve Web3 integration. In Table 1, all the components and technologies of BCTVCO are listed out.

Table 1. Summary of tools and technologies

Component	Technology used
Consensus algorithm	PoS
Block chain development environment	Local Hardhat Node
Smart contract compilation and deployment	Remix IDE
Frontend framework	React.js
Blockchain wallet	MetaMask

DataSet*:* the evaluation in this work uses a synthetic dataset generated through simulated social media interactions. A group of virtual users is created to act as content creators, re-sharers, and auditors. Each simulated action in the system automatically generates a blockchain transaction, enabling evaluation without the need for an external dataset. Each transaction record consists of the following fields:

- Content Hash-unique SHA-256 fingerprint of uploaded content.
- User ID-pseudonymous identity of the participating user.
- Timestamp-time of upload, sharing, or audit.
- Interaction Type-create, share, edit, verify, or audit.
- Platform Tag-simulated platform used for dissemination.

This controlled dataset allows us to analyze tracking delay, storage growth, and user participation trends as the number of transactions increases. In future work, we plan to validate BCTVCO using real social media datasets and large-scale user interactions to test the practical deployment of the system.

Scalability and Cost Considerations: Unlike public Ethereum mainnet deployments, BCTVCO utilizes a private PoS blockchain, eliminating high gas fees. Only hash-level metadata is stored on-chain, while bulk content resides on IPFS, which significantly reduces blockchain storage costs. Future work includes deploying BCTVCO over low-cost layer-2 networks such as Polygon and BSC to ensure cost-efficient and scalable operation during mass adoption.

In Figure 2, the graph indicates a linear rise in tracking time, indicating that the system takes longer to track the origin of content as more transactions take place. In Figure 3, transaction validation is evaluated. The time across nodes boxplot illustrates the variation in validation time among three distinct nodes in a blockchain network. Three distinct nodes (nodes 1, 2, and 3) are represented by the X-axis (nodes) in this. The time required for transaction validation at each node is shown on the Y-axis (validation time in ms).

The interquartile range (IQR), which is represented by the boxes, indicates the range of validation times. The median validation time is shown by the horizontal line inside the box. The validation times for each of the three nodes are quite comparable. Node 3 has a slightly lower maximum validation time (~30 ms), while Node 2 has the greatest (~35 ms). The median validation times are close to 20 mms across all nodes, showing a relatively stable transaction processing time.

In Figure 4, the accuracy of content origin is evaluated for tracing as a function of tracing time delay, is seen in this scatter plot. The time required to track down the content's original source is shown on the X-axis (time delay in seconds). The accuracy of identifying the content's original source is represented by the Y-axis (accuracy in percentage). The accuracy of content origin tracing declines with increasing time delay. Accuracy is 99% at 1 second delay, suggesting almost flawless tracking. Accuracy decreases to 89% after 5 seconds of delay, demonstrating how delays impair tracking precision. This declining trend implies that more accurate findings come from faster content tracking.

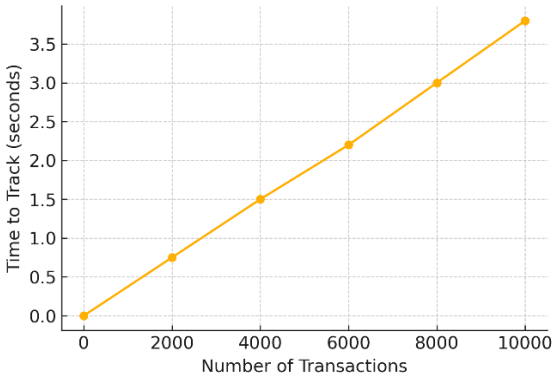

Figure 2. Content origin tracking time growth

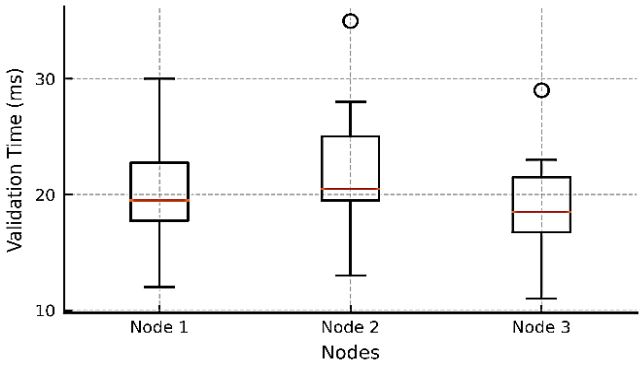

Figure 3. Transaction validation

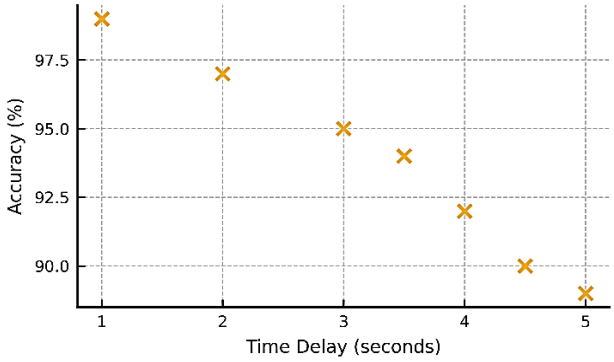

Figure 4. Accuracy of content origin

In Figure 5, the Consensus algorithm evaluates the efficacy of several blockchain consensus algorithms for locating the sources of viral material on social media. While PoS (~90%) and DPoS (~85%) perform better with increased efficiency, PoW has the lowest efficacy (~65%) due to its slower transaction speed and greater computing expenses. PBFT (~80%) provides speedier consensus and is frequently used in permissioned networks. Due to its particular architecture for tracking viral content, which probably includes efficient data verification, streamlined consensus processes, and interaction with IPFS for decentralized storage, BCTVCO achieves the maximum effectiveness (~95%).

In Figure 6, the scalability of several blockchain consensus methods: proof of work (PoW), PoS, delegated proof of stake (DPoS), practical byzantine fault tolerance (PBFT), and BCTVCO is expressed in transactions per second (TPS). PoS (~50 TPS) and DPoS (~100 TPS) demonstrate benefits by lowering energy consumption and boosting efficiency, whereas PoW has the lowest scalability because of its computationally demanding mining process. Because it requires consensus among a predetermined selection of nodes rather than mining, PBFT (~200 TPS) performs better. With the greatest TPS (~300), BCTVCO performs better than the others, most likely as a result of its streamlined consensus process created especially for tracking viral material.

In Figure 7 user participation in auditing comparison evaluates and contrasts the percentage of users who participated in audits across various blockchain consensus algorithms. The y-axis shows the proportion of people actively participating in audits, while the x-axis depicts several consensus mechanisms—PoW, DPoS, PBFT, and BCTVCO. Because PoW relies more on mining than on direct auditing, it has the lowest user engagement rate (~30%). While PBFT (~78%) generates even higher involvement by needing validator agreement, DPoS (~60%) increases participation by letting users vote for delegates. The reason BCTVCO has the highest participation rate (around 80%) is probably because it was created specifically to track viral material, and auditing is an essential component of its verification procedure. The evaluation presented in this work uses a controlled experimental setup with synthetic interaction logs generated through simulated content sharing and auditing behavior. This dataset allows us to empirically analyze scalability, storage growth, and tracking delay under increasing load. Although the results demonstrate feasibility and operational efficiency, integration with major social media platforms and real-world datasets is planned as part of future development. Such deployment will enable validation in practical environments with large-scale user interactions, diverse content types, and real propagation patterns.

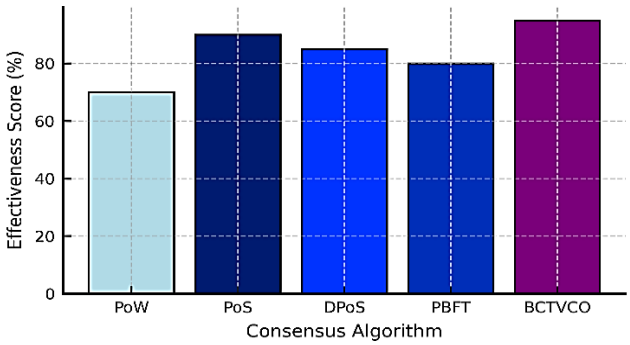

Figure 5. Effectiveness score consensus algorithm

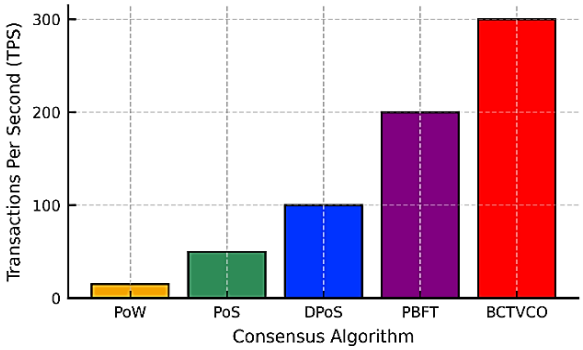

Figure 6. Scalability of a blockchain-based system

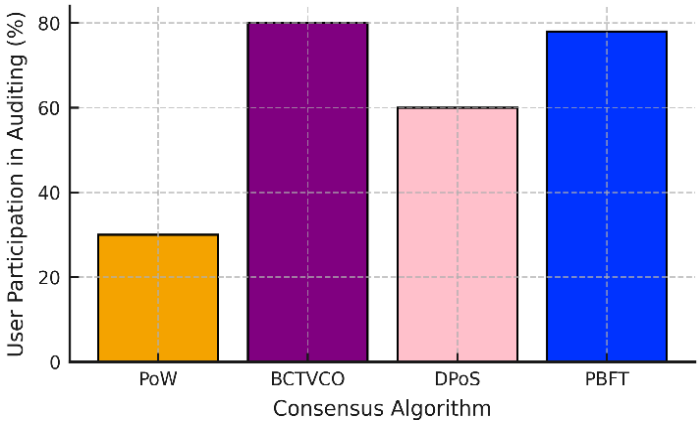

Figure 7. User participation in auditing comparison

4. CONCLUSION

In contrast to conventional verification techniques that depend on external enforcement and centralized repositories. Here, the proposed system BCTVCO uses IPFS for decentralized storage, Ethereum smart contracts for ownership tracking, and SHA-256 hashing for content fingerprinting. This gives content providers a safe and scalable solution by removing the risks related to censorship, manipulation, and single points of failure. The benefits of blockchain-based ownership tracking are highlighted by comparisons with traditional digital rights management (DRM). AI-powered verification and decentralized storage, especially in terms of automated detection, tamper-proof verification, and fast notifications. Our approach offers a cryptographically secure and deterministic substitute for conventional authentication methods, which frequently have significant false-positive rates and manual oversight. The next-generation Web3 ecosystem is made possible by this system, which strengthens digital content security and copyright protection by combining blockchain technology, decentralized storage, and sophisticated fraud detection techniques. In future work, we plan to evaluate the system using real social media datasets and large-scale user interactions to validate its practical deployment.

FUNDING INFORMATION

No funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Nageswararao Sirisala	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Srinivasulu Sirisala	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓		
Nalavala Ramanjaneya Reddy	✓	✓				✓			✓		✓		✓	
Syed Anisha			✓	✓	✓		✓	✓		✓				

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

Data availability does not apply to this paper, as no new data were created or analyzed in this study.

REFERENCES

[1] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," *in Proc. IEEE 5th Int. Conf. Big Data and Cloud Computing*, Dalian, China, 2015, pp. 187–190, doi: 10.1109/BDCloud.2015.60.

[2] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, "Fake news detection on social media: a data mining perspective," *ACM SIGKDD Explorations Newsletter*, vol. 19, no. 1, pp. 22–36, Sept. 2017, doi: 10.1145/3137597.3137600.

[3] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.

[4] C. Li and B. Palanisamy, "Incentivized blockchain-based social media platforms: a case study of Steemit," *in Proc. 10th ACM Conf. Web Science*, 2019, doi: 10.1145/3292522.3326041.

[5] S. Mekala, T. N. S. Padma, and R. R. Tandu, "DHM-OCR: a deep hybrid model for online course recommendation and sustainable development of education," *International Journal of Electrical and Computer Engineering Systems*, vol. 15, no. 4, pp. 345–354, 2024, doi: 10.32985/ijeces.15.4.5.

[6] D. Raj and D. Sharma, "Enhancing digital image forensics and security: innovations in metadata, watermarking and blockchain technology," in *Proc. OPJU Int. Technology Conf. (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, Raigarh, India, 2024, pp. 1–6, doi: 10.1109/OTCON60325.2024.10688307.

[7] L. Widick, I. Ranasinghe, R. Dantu, and S. Jonnada, "Blockchain based authentication and authorization framework for remote collaboration systems," in *Proc. IEEE 20th Int. Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Washington, DC, USA, 2019, pp. 1–7, doi: 10.1109/WoWMoM.2019.8792994.

[8] S. Sirisala, N. Sirisala, and G. Rajeswarappa, "Eigen vector based trust model (EVTM) for ensuring quality of service (QoS) in Mobile Ad Hoc Networks," *International Journal of Computer Networks and Applications*, vol. 11, no. 3, p. 351, Jun. 2024, doi: 10.22247/ijcna/2024/22.

[9] V. S. T. Reddy, S. Parvathi, C. Sarada, K. H. Mohmmed, A. S. D. Murthy, and K. Saikumar, "Enterprise support hierarchical model with secure data protocol," in *Proc. 3rd Int. Conf. Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 2023, pp. 1–6, doi: 10.1109/SMARTGENCON60755.2023.10442282.

[10] S. Lalitha and K. Sooda, "DeepFake detection through key video frame extraction using GAN," in *Proc. Int. Conf. Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, 2022, pp. 859–863, doi: 10.1109/ICACRS55517.2022.10029095.

[11] S. Sirisala and S. R. Krishna, "Fuzzy COPRAS-based node cooperation enforcing trust estimation scheme for enhancing quality of service (QoS) during reliable data dissemination in MANETs," *International Journal of Communication Systems*, vol. 34, no. 7, e4767, 2021, doi: 10.1002/dac.4767.

[12] Y. Zhang, C. Xu, and X. Wang, "AI-powered fake content detection: challenges and future directions," *IEEE Access*, vol. 10, pp. 67823–67840, 2022, doi: 10.1109/ACCESS.2022.3186580.

[13] H. Zhang, Y. Chen, and J. Zhang, "Fake image and video detection using AI and blockchain technologies," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 5, pp. 2091–2105, 2022, doi: 10.1109/TNNLS.2021.3052044.

[14] A. Shahzad, W. Chen, Y. Zhang, and R. Kumar, "Zero-trust medical image sharing: a secure and decentralized approach using blockchain and the IPFS," *Symmetry*, vol. 17, p. 551, 2025, doi: 10.3390/sym17040551.

[15] S. Dhall, A. D. Dwivedi, S. K. Pal, and G. Srivastava, "Blockchain-based framework for reducing fake or vicious news spread on social media/messaging platforms," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 21, no. 1, Art. no. 8, 2022, doi: 10.1145/3467019.

[16] F. Frattolillo, "Blockchain and smart contracts for digital copyright protection," *Future Internet*, vol. 16, p. 169, 2024, doi: 10.3390/fi16050169.

[17] N. Sirisala and C. Bindu, "A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 116–125, Apr. 2017, doi: 10.22266/ijies2017.0430.13.

[18] Q. Chen, Y. Kong, and L. Cheng, "A digital copyright protection system based on blockchain and with sharding network," in *Proc. IEEE 10th Int. Conf. Cyber Security and Cloud Computing (CSCloud)/IEEE 9th Int. Conf. Edge Computing and Scalable Cloud (EdgeCom)*, Xiangtan, Hunan, China, 2023, pp. 393–398, doi: 10.1109/CSCloud-EdgeCom58631.2023.00073.

[19] F. Bassan and M. Rabitti, "From smart legal contracts to contracts on blockchain: an empirical investigation," *Computer Law & Security Review*, vol. 55, p. 106035, 2024, doi: 10.1016/j.clsr.2024.106035.

[20] N. Sangeeta and S. Y. Nam, "Blockchain and interplanetary file system (IPFS)-based data storage system for vehicular networks with keyword search capability," *Electronics*, vol. 12, p. 1545, 2023, doi: 10.3390/electronics12071545.

[21] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security and Privacy Workshops*, San Jose, CA, USA, 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.

[22] N. Nizamuddin, K. Salah, M. A. Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, pp. 183–197, 2019, doi: 10.1016/j.compeleceng.2019.03.014.

[23] N. Sirisala, A. Yarava, Y. C. A. P. Reddy, and P. Veeresh, "A novel trust recommendation model in online social networks using soft computing methods," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 22, e7281, 2022, doi: 10.1002/cpe.7281.

[24] M. John, V. B. Ambhore, C. Karthikeyan, M. Gupta, P. Chandrakala, and A. Garg, "Improving trust management in IoT-edge networks with blockchain and enhanced ETEE approach for Sybil attack reduction," *in Proc. IEEE 4th Int. Conf. ICT in Business Industry & Government (ICTBIG)*, Indore, India, 2024, pp. 1–6, doi: 10.1109/ICTBIG64922.2024.10911513.

[25] A. Elgalaly, A. Fahmy, A. Ahmed, M. Youssif, M. Essam, and S. A. E. Mohamed, "Blockchain-driven defense against deepfakes on social media platforms," *in Proc. 12th Int. Japan-Africa Conf. Electronics, Communications, and Computations (JAC-ECC)*, Alexandria, Egypt, 2024, pp. 170–175, doi: 10.1109/JAC-ECC64419.2024.11061235.

[26] R. Li, Y. Sun, C. Liu, Y. Wen, and Y. Liu, "Distributed data sharing and access control in industrial IoT using blockchain technology," *in Proc. 5th Int. Conf. Computer Engineering and Intelligent Control (ICCEIC)*, Guangzhou, China, 2024, pp. 372–375, doi: 10.1109/ICCEIC64099.2024.10775761.

BIOGRAPHIES OF AUTHORS

Dr. Nageswararao Sirisala has received Ph.D. in the Dept. of Computer Science and Engineering (CSE), from JNT University Anantapuramu, AP, India. He has published more than 20 research papers in international conferences and journals. His area of interest is mobile ad-hoc networks, algorithms, and soft computing methods. He can be contacted at email: nagsirisala@gmail.com.

Dr. Srinivasulu Sirisala has completed his Ph.D. in Computer Science from Sri Venkateswara University, Tirupati. He has published more than 12 papers in international, national journals. His Current area of interest includes manets, artificial learning, and machine learning. He can be contacted at email: vasusirisala@gmail.com.

Dr. Nalavala Ramanjaneya Reddy has completed his Ph.D. in CSE, from JNTUA, Ananthapuramu. He has more than 14 years of teaching experience and he published many research papers in reputed national and international journals. Also, he obtained patents on his work. His research areas include computer networks, data science, and artificial intelligence. He can be contacted at email: nalavala.ramanji@gmail.com.

Syed Anisha currently studying M.Tech. in KLM College of Engineering for Women, she had completed my B.Tech. in the specialization of Computer Science and in Engineering (CSE) in KSRM College of Engineering (Autonomous), Kadapa, Andhra Pradesh, India. Her research areas of intrest are blockchain technology, machine learning, and Python. She can be contacted at email: anishasyed465@gmail.com.