International Journal of Science and Engineering Applications
Volume 14-Issue 06, 34 – 38, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1406.1006

Integrating Blockchain and Artificial Intelligence: A Secure Framework for Data Integrity, Decentralized Applications, and Digital Transformation

Salson Martin
Department of Computer Science
Centurion University
Paralakhemundi, Odisha, India

Arif Mohammad
Department of Computer Science
Centurion University
Paralakhemundi, Odisha, India

Naga Harsha Tumma
Department of Computer Science
Centurion University
Paralakhemundi, Odisha, India

Abstract: The convergence of blockchain and artificial intelligence (AI) is revolutionizing secure data management and intelligent decision-making across industries. This paper investigates the transformative potential of integrating blockchain's immutable, decentralized ledger systems with AI's predictive and cognitive capabilities. Through comprehensive literature synthesis and analysis, the study highlights how AI enhances the efficiency of smart contract execution and decision-making while blockchain fortifies data provenance, authentication, and security. Applications in healthcare, supply chains, financial systems, and the Internet of Things (IoT) are examined, emphasizing the dual benefits of transparency and automation. The paper discusses decentralized identity systems, fraud detection, compliance assurance, and ethical concerns surrounding this integration. A blockchain-AI hybrid framework is proposed to support tamper-proof data integrity, enhance cybersecurity, and optimize industrial processes. Future directions suggest the necessity of establishing global standards and ethical protocols to realize the full potential of this synergy. The study concludes that the AI-blockchain fusion is a cornerstone for next-generation secure digital ecosystems.

Keywords: Blockchain Technology; Artificial Intelligence; Data Integrity; Smart Contracts; Cybersecurity; Decentralized Applications; Supply Chain Transparency

1. INTRODUCTION

WAI technology returns in new usages due to blockchain, which is assisted by high-level security and data keeping features of its proven data integrity achievement computing capability. Transactions from the blockchain system and smart contract execution also happen more efficiently because of AI nodes that run at the blockchain infrastructure level [1]. The studies found show that integration with an AI tool and another tool of blockchain can create new bounds of applications in the field [3]. Blockchain technology-based combined system further boosts business system modification and gives customer interaction more effectively, as stated in the literature source [6]. This has true values due to various data distribution techniques for allowing extensive data distribution pathways as specified by [2] as a result of implementing blockchain with AI systems. A blockchain-based system acting as the original source for data serves for the trustful authentication of AI data sets through management techniques based on [4] intrusion encryption. Data management systems are decentralized because Blockchain technology integrates AI to create infrastructure that allows the distributed deployment of AI applications [5]. New research on the right way to merge AI and blockchain has to emerge since scientists currently do not have enough knowledge about this new borderline field of combined deployment [16]. Users gain the integration of such artificial intelligence technology into the blockchain to change the data and create a new way of standardizing system management [8]. Today, companies have to apply self-management systems as they satisfy critical requirements of their organizational framework [7]. This change emanates from technological progress, the knowledge growth, and the acquisition of new skills as stated by [9]. Blockchain technology is going to merge with artificial intelligence, and it is going to push the business model development at a faster pace in the coming years [10].

The addition of the tagline of AI and blockchain can give rise to safe servers for the possible present electronic interoperability and data governance exchange of digital prints [11]. An area where blockchain may provide more security and one point of evident privacy of vaulting the data is in the creation of decentralized people [12]. Figure 1 shows the uses of Blockchain and AI systems.

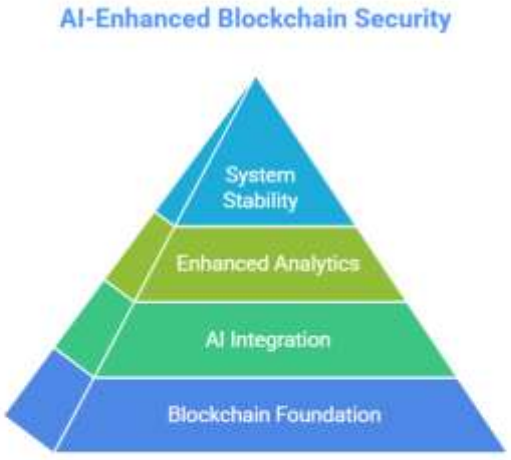

Figure 1: Security enhancement using Blockchain and AI systems

Self-sovereign identities generated out-of-blockchain enable users to manage their digital identity buried in the self-contained dataset and share only what they wish [13]. The connected systems can be made stable, reliable, trustworthy, and secure by translating the Organization into characteristics of Distributed and Irreversible blockchain, by merging the qualities of AI, which is able to comprehend, learn, and execute decisions to enhance analytics [14].

The creation of decentralized, transparent, mundane-to-hacking systems may be recognized as one of the huge positive aspects of integrating AI and smart contracts on the blockchain [15]. Blockchain is decentralized on its own, which means it is not controlled by any single company. Because of the decentralized nature of blockchain, it verifies the facts of a transaction to complete the transaction on behalf of the user [16]. Blockchain might move outside of data-rich change in numerous sectors, by providing more protection as well as transparency [19]. By integrating AI into blockchain, businesses will possess a much more secure and efficient means for their systems to operate effectively [20]. The combination of AI and blockchain in business development is still needed, and further research steps are needed [17].

2. BLOCKCHAIN-DRIVEN ADVANCES IN HEALTH INFORMATION MANAGEMENT

The implementation of Blockchain enables Walmart and similar organizations to strengthen their supply chain functions for food protection [14]. The Grand View Research study shows blockchain will grow to reach $394.6 billion during the years from 2028 to 2038 [15]. The implementation of Blockchain technology allows organizations to develop data management systems that employ protective procedures following the description from [16]. The instant availability of business system issues combines with blockchain identification of ongoing fraud via its transparent data system, which likewise detects manufacturing delays [18]. Blockchain systems enable supply chain participants to see all operations to develop strong relationships based on trust, which leads to better workplace cooperation [21]. Blockchains enable supply chains to develop new capabilities through enabling complete trackable visibility between supply chain partners [17]. Businesses extend their contract development period through smart contracts, which execute independent complex procedures automatically without requiring middle actors for intervention [29].

The growing demands from consumers create excellent conditions for companies to develop sustainable programs utilizing fair trade criteria alongside open transparency programs [5]. Blockchain uses an associative structure for real-time information updates, so businesses no longer need to submit reports, as noted in [18]. Business organizations adopt blockchain technology to establish verification platforms that support their sustainable business practices and maintain ethical operational standards [18]. Developing countries need to put Blockchain technology into practice because this technological system blocks counterfeit and substandard products from reaching the market [19]. Blockchain solutions enable companies to track their supply chain products across their network for absolute tracking, complete product tracing, and transparent transaction monitoring [10,11]. Effective access to customer services emerges through supply chain development that integrates dependable information systems [12].

The merger of Blockchain technology and AI produces major system transitions that assist modern financial establishments in combating money laundering and improving customer care systems [27]. The implementation of blockchain technology allows pharmaceutical industries to investigate counterfeit drugs across their distribution networks through their system infrastructure [7]. Businesses achieve operational problem solutions alongside supply chain transparency from blockchain technology using AI operational management systems, according to 27 and 13. Through its AI algorithmic system, the system analyzes large transaction databases to detect abnormal patterns in behavioral sequences and provide time-critical monitoring functions [27]. The combination of Blockchain-AI technology allows financial organizations to enhance operational performance and reduce costs, which produces superior security features and rapid, secure information handling mechanisms [27]. The successful connection between blockchain and artificial intelligence depends on problem solutions that establish adequate network communication standards according to [27]. Blockchain technology uses secure information protection structures based on encryption systems that implement cryptographic hash methods as described in [27]. Blockchain activates cryptographic protocols that execute protection throughout their entire processing period by defending transactions and preventing fraudulent activities. [25,27,22,30].

Public transaction transparency in blockchain systems exists because blockchain operations create complete traceability of transactions as described in [10]. Organizations that use the Quorum blockchain framework can perform KYC checks, which improves their media system operations [27]. Medical facilities enhance system protection through blockchain technology while gaining decentralized operation capabilities to defend themselves against extensive threats [10]. Medical information access provided to patients through AI and blockchain technology results in secure information viewing for operational improvement and data protection [10, 19]. The operational trust of clinical research teams within medical trial automation grows because their partnership with the AI blockchain enables the fulfillment of patient privacy standards [30]. The healthcare blockchain system performs two main operations, which include protecting medical records along with medication tracking data, while providing medical information transfers as the core linking mechanism between different healthcare facilities. A blockchain network's intrinsic qualities, decentralization, immutability, and transparency, make it well-suited for the safe and effective exchange of medical data. Healthcare sectors that reach maximum efficiency through blockchain systems are able to protect patient data securely while ensuring complete confidentiality, which drives down healthcare financial expenses. The research document is available in its entirety by checking [10], [15], [16], and [25].

Blockchain enables voting systems to merge security safeguards with transparent features to establish powerful democratic systems that decrease incidents of election fraud [25]. IoT service delivery platforms team up with blockchain technologies to create secure network services for their devices [21]. Figure 2 shows the uses of IoT and Blockchain to enhance the system.

Internet of Things systems have become useful for public security systems through blockchain security flaw detection technology, which unites data collection functions to get critical case information [14]. The secure digital application connections of the modern era must implement blockchain technology as their core building component.

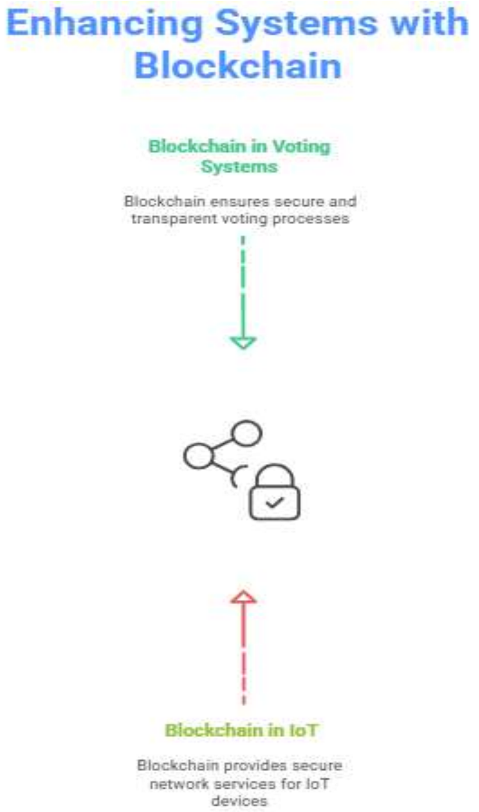
Enhancing Systems with Blockchain
Blockchain in Voting Systems
Blockchain ensures secure and transparent voting processes
Blockchain in IoT
Blockchain provides secure network services for IoT devices

Figure 2: IoT and Blockchain to enhance the system.

The protective nature of Blockchain consists of three fundamental abilities: authenticating crypto systems, deploying decentralized systems and consensus frameworks, and establishing smart contracts, together with additional optional features [29]. The implementation of blockchain technology in Internet of Things systems generates separate security concerns originating from cyberspace assaults alongside data management hurdles [15]. Blockchain transaction protection utilizes authenticating protocols that work together with key encryption methods alongside signature and hash implementations, as explained by [29]. This system implements security features that define boundaries to stop attacks against blockchain platform data [29]. According to the information provided in [29], risk control approaches function as core components for delivering safe distributed information.

3. BLOCKCHAIN-BASED FRAMEWORKS FOR DATA INTEGRITY ENFORCEMENT

Typically, blockchain innovation is desirable for time-buffering data exchanges in various industrial domains [30]. The AI and blockchain in the financial sector refers to mutual understanding between the common world, regulatory relationships, compliance barriers, and technology obstacles [27]. AI can be combined to aid risk-takers, fraud detection and compliance, data integrity, and safety enforced by blockchain [27]. By driving innovation and protecting consumers and the financial system, the financial staff can leverage these ideas to understand the challenges of parenting AI and Blockchain [27]. But for that to occur, banks must expend so heavily on some serious R&D effort as well as on human resources and infrastructure [19]. The pairing of blockchain and AI results in the security of data transactions and the increased harmonization of operations across a number of areas. The AI-blockchain venture must have fraud detection to run, needs, and customer service that has automated functions [27]. It should be noted that the AI is used for this purpose, and the risk will be lower fraud detection, regulatory improvement [27, 17], and blockchain provides data confidentiality and integrity. Adding it [30] to the lift of AI gives the security, comfort & efficiency of the blockchain. AI blockchain technology is the AI technology that employs ML technology to perform a large collection of work and actions by integration [29].

The combination of artificial intelligence systems and blockchain operations within financial tools leads to a significant transformation of the entire financial industry [18]. The rapid spread of blockchain technology with AI systems requires an essential ethical control system because of their quick adaptation speed [22]. Modern innovative platforms generate operational changes that improve business performance within their specific business domains [23]. The combination of AI and blockchain technology brings organizations essential cybersecurity benefits, which help them detect threats in secure system development operations [19]. Security protocols based on blocking technology operate distributed ledgers to provide essential protection mechanisms that maintain safety and confidentiality through all interactions with external entities [24]. The real-time monitoring capabilities with complex analytical features in systems result in enhancing operational performance for cybersecurity threat prevention. Organizations obtain data security through combining blockchain technology with AI operational integration [13].

The implementation of AI technology with blockchain systems by financial companies allows these institutions to achieve multiple operational modifications that enhance data source management, as noted by [27]. The system enables organizations to forecast market potential during their business launch through these running algorithms. The automatic blocking system gains improved capabilities for fraud detection by running constant AI algorithm applications that monitor suspicious activities [25]. The operational capability of blockchain networks increases because programmed agreements give blockchain platforms access to specific blockchain data according to [26]. The integration of smart contracts with AI-based platform control systems delivers an extended fraud prevention method for protecting data security and stopping unauthorized network access [27]. Traditional contract deployment operations allow users to generate better smart contracts using improved AI functions through User applications [28]. Infrastructure platforms develop AI systems with the help of blockchain technology by implementing certain recommendation methods [29].

The integration of blockchain technology into decentralized security structures permits the identification of potential industrial security breaches because blockchain-based assaults become impossible [26]. Blockchain networks use their distributed server approach to distribute safety procedures that stop both unauthorized modifications and technical faults [31]. Absolute tamperproof protection allows automated blockchain systems to grow trust potential by implementing oversight procedures for automated systems. Blockchain defense systems implement three separate protocols to protect electronic transactions by blocking unauthorized data modification in open system-generated records. The data security mechanism of public blockchain maintains data integrity by executing two operational security protocols and cryptographic algorithms. Organizations achieve decreased operational expenses in their back-end business regions through cryptography-based approaches [27].

The smart Blockchain system helps organizations create protected networks that enable them to advance their operational excellence achievements in the current industrial revolution. As part of his work, Hanson supports system developers in developing disruptive solutions that enhance the decision analysis systems' performance quality alongside automated programming models [28]. Programming algorithms serve as fundamental implementation tools that enable system development for computer-based AI systems to assess data during all development periods for accurate specification execution. The peak performance level of modern business solutions emerges from integrating advanced anti-fraud and anti-cyber threat technology through an artificial intelligence and machine learning framework, smart contract connections [17, 29]. Modern technological systems facilitate quality control systems to create dependable linkages that lead to successful industrial outputs. Recommendation systems help organizations begin recommended conditions through the following protocols, which are described in [30]. The functionality of blockchains improves because artificial intelligence systems perform qualitative assessments of transactional and smart contract system databases. References 34 and 38 explain these findings.

4. CURRENT LIMITATIONS AND FUTURE PROSPECTIVE ADVANCES

The privacy configuration used at the completion of technical development remains in effect right through to the conclusion of the standardization phase. Industrial adoption of blockchain technology demands novel solutions for performance improvement and security standards to reach operational connectivity. The establishment of standardized procedures must come first before supply chain problems can be solved for consumer safety improvements to be successful. Scientific research is required to prove and validate every advantage related to integrating AI systems with blockchain technology [30].

The methodology supports the development of critical operational benefits that recommend data integrity specifications for health supply chain management systems. Users need to enable verification protocols based on blockchain protocols when they modify database entries to achieve security across all connected systems [21]. The tamper-evident nature of blockchain ensures maximum transparency, according to [28]. Blockchains achieve permanent data storage through operations since their system prevents any modifications [30]. All members of this system gain transparent, open access to transactions with no need for intermediary service [20].

5. CONCLUSION

The integration of blockchain technology and artificial intelligence (AI) presents a transformative pathway for enhancing security, transparency, and operational efficiency across multiple sectors. By leveraging the decentralized, immutable nature of blockchain alongside AI’s adaptive and predictive capabilities, organizations can establish robust infrastructures for secure data management, automated decision-making, and fraud prevention. The combined framework offers significant benefits in domains such as healthcare, financial systems, supply chain management, and IoT, ensuring real-time monitoring, trustworthy analytics, and streamlined processes. Despite its vast potential, the implementation of this synergy requires the development of ethical standards, regulatory frameworks, and interoperability protocols to address privacy, scalability, and compliance challenges. As industries move toward increasingly digital and data-driven models, the AI-blockchain convergence will serve as a foundational pillar for constructing resilient, intelligent, and future-ready ecosystems.

6. REFERENCES

[1]. Almanasir, R., Al-solomon, D., Indrawes, S., Amin Almaiah, M., Islam, U., & Alshar’e, M. (2025). Classification of threats and countermeasures of cloud computing. Journal of Cyber Security and Risk Auditing, 2025(2), 27–42. https://doi.org/10.63180/jcsra.thestap.2025.2.3

[2]. Kasula, V. (2024). Leveraging Deep Learning Techniques for Enhancing Financial Security Systems: A Comprehensive Review of Methods, Applications, and Challenges. International Journal of Communication Networks and Information Security (IJCNIS), 16(5), 969–978.

[3]. Kumar, D., Pawar, P. P., Ananthan, B., Indhumathi, S., & Murugan, M. S. (2024, May). CHOS_LSTM: Chebyshev Osprey optimization-based model for detecting attacks. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.

[4]. Addula, S. R., Mamodiya, U., Jiang, W., & Almaiah, M. A. (2025). Generative AI-Enhanced Intrusion Detection Framework for Secure Healthcare Networks in MANETs. SHIFRA, 2025, 62-68.

[5]. A. Al-Shareeda, M., Mohammed Ali, A., Adel Hammoud, M., Haider Muhammad Kazem, Z., & Aqeel Hussein, M. (2025). Secure IoT-Based Real-Time Water Level Monitoring System Using ESP32 for Critical Infrastructure. Journal of Cyber Security and Risk Auditing, 2025(2), 44–52. https://doi.org/10.63180/jcsra.thestap.2025.2.4

[6]. S. Almotairi et al., “Personal data protection model in IOMT-blockchain on secured bit-count transmutation data encryption approach,” Fusion: Practice and Applications, vol. 16, no. 1, pp. 152–170, 2024. doi:10.54216/fpa.160111

[7]. Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Beyond the Horizon: Drone-Assisted HAR Through Cutting-Edge Caps Net and Optimization Techniques. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.

[8]. Pawar, P. P., Kumar, D., Ananthan, B., Christopher, S. B., & Surya, R. (2024, May). An advanced Wasserstein-enabled generative adversarial network enables attack detection for blockchain-assisted Intelligent Transportation systems. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.

[9]. V. K. Kasula et al., "Federated Learning with Secure Aggregation for Privacy-Preserving Deep Learning in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-7, doi: 10.1109/ICCA65395.2025.11011120.

[10]. M. Yenugula et al., "A Graph Neural Diffusion Network for Sophisticated Persistent Threat Hunting in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-6, doi: 10.1109/ICCA65395.2025.11011108.

[11]. A. R. Yadulla et al., "Lightweight Neural Networks for Adversarial Defense: A Novel NTK-Guided Pruning Approach," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 331-337, doi: 10.23919/FRUCT65909.2025.11008002.

[12]. V. K. Kasula et al., "An improved machine learning technique for credit card fraud detection," Edelweiss Appl. Sci. Technol., vol. 9, no. 5, pp. 3093–3109, 2025.

[13]. Manoj, H. M., Pawar, P. P., Krupa, R., Pareek, P. K., Kumar, D., & Bandeppa, L. (2024, July). PFCM-based Segmentation and TFA-based DCNN model for Skin Cancer Classification using Dermoscopic Images. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-7). IEEE.

[14]. Menon, S., Addula, S. R., Parkavi, A., Subbalakshmi, C., Dhandayuthapani, V. B., Pokkuluri, K. S., & Soni, A. (2024). Streamlining Task Planning Systems for Improved Enactment in Contemporary Computing Surroundings. SN Computer Science, 5(8), 993.

[15]. Kumar, N., et al. (2025). Advanced banking solutions for Industry 5.0: From industry's perspective. In Creating AI synergy through business technology transformation (pp. 1–24). IGI Global.

[16]. Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. S., & Selvi, A. S. (2024, May). An efficient DDoS attack detection using an attention-based hybrid model in blockchain-based SDN-IOT. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE.

[17]. Misra, N. K., et al. (2024). COVID-19 pandemic: A worldwide critical review with the machine learning model-based prediction. Journal of The Institution of Engineers (India): Series B, 1–11.

[18]. Kumar, N., et al. (2025). Advanced banking solutions for Industry 5.0: From industry's perspective. In Creating AI synergy through business technology transformation (pp. 1–24). IGI Global.

[19]. Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Arithmetic Optimized Bi-GRU: A Swift Approach to Combat Fake News in the Digital Sphere. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.

[20]. Pawar, P. P., Kumar, D., Krupa, R., Pareek, P. K., Manoj, H. M., & Deepika, K. S. (2024, July). SINN Based Federated Learning Model for Intrusion Detection with Blockchain Technology in Digital Forensic. In 2024 International Conference on Data Science and Network Security (ICDSNS)(pp. 01-07). IEEE.

[21]. Kumar, D., Pawar, P. P., Ananthan, B., Rajasekaran, S., & Prabhakaran, T. V. (2024, May). Optimized support vector machine-based fused IOT network security management. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE.

[22]. Daniel, V. A. A., Vijayalakshmi, K., Pawar, P. P., Kumar, D., Bhuvanesh, A., & Christilda, A. J. (2024). Enhanced affinity propagation clustering with a modified extreme learning machine for segmentation and classification of hyperspectral imaging. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 9, 100704.

[23]. Vadakkethil, S. E., Polimetla, K., Alsalami, Z., Pareek, P. K., & Kumar, D. (2024, April). Mayfly Optimization Algorithm with Bidirectional Long-Short Term Memory for Intrusion Detection System in Internet of Things. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.

[24]. C. Tumma et al., "Data Security and Privacy Protection in Artificial Intelligence Models: Challenges and Defense Mechanisms," Int. J. Sci. Res. Eng. Manag., vol. 7, no. 12, pp. 1–11, 2022.

[25]. S. Ayyamgari et al., "Quantum Computing: Challenges and Future Directions," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 3, pp. 1343–1347, 2023.

[26]. B. Y. R. Thumma et al., "Cloud Security Challenges and Future Research Directions," Int. Res. J. Mod. Eng. Technol. Sci., vol. 4, no. 12, pp. 2157–2162, 2022.

[27]. R. Azmeera et al., "Enhancing blockchain communication with named data networking: A novel node model and information transmission mechanism," J. Recent Trends Comput. Sci. Eng. (JRTCSE), vol. 10, no. 1, pp. 35–53, 2022.

[28]. V. K. Kasula et al., "Enhancing Hyperledger Fabric Security with Lightweight Post-Quantum Cryptography and National Cryptographic Algorithms," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 93-99, doi: 10.23919/FRUCT65909.2025.11008110.

[29]. A. R. Yadulla et al., "Enhanced Cybersecurity Entity Recognition Using DeBERTa, Transformer-CNN Hybrids, and BiLSTM-Softmax," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 323-330, doi: 10.23919/FRUCT65909.2025.11008057.

[30]. B. Konda et al., "Enhancing Traceability and Security in mHealth Systems: A Proximal Policy Optimization-Based Multi-Authority Attribute-Based Encryption Approach," 2025 29th International Conference on Information Technology (IT), Zabljak, Montenegro, 2025, pp. 1-6, doi: 10.1109/IT64745.2025.10930307.

[31]. P. Pawar et al., "Exploring Blockchain-Enabled Secure Storage and Trusted Data Sharing Mechanisms in IoT Systems," 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2025, pp. 1-6, doi: 10.1109/IATMSI64286.2025.10984499.