The Eastasouth Journal of Information System and Computer Science
Vol. 4, No. 01, August 2026, pp. 17-28
ISSN: 3025-566X, DOI: 10.58812/esiscs.v4i01

Blockchain-Driven Cybersecurity Framework for Smart Digital Ecosystems

Marion Kayla[1], Crispinus Ode[2], Marion Sanaipei[3]
[1,2,3] Independent Researcher, Ontario, Canada

Article Info

Article history:

Received June, 2026
Revised July, 2026
Accepted Aug, 2026

Keywords:

Artificial Intelligence;
Blockchain;
Cloud Security;
Consensus Mechanisms;
Cybersecurity;
Decentralized Security;
Edge Computing;
Internet of Things;
Intrusion Detection Systems;
Smart Digital Environments

ABSTRACT

The rapid growth of smart digital environments, driven by cloud computing, the Internet of Things (IoT), artificial intelligence (AI), and interconnected cyber-physical systems, has significantly increased the frequency and sophistication of cyber threats. Conventional cybersecurity approaches often struggle to ensure data integrity, trust, and resilience in decentralized and highly dynamic environments, highlighting the need for more robust security frameworks. This review paper examines the role of blockchain technology in enhancing cybersecurity for smart digital ecosystems through decentralized authentication, immutable data storage, secure information sharing, and intelligent threat mitigation. The study reviews blockchain architectures, consensus mechanisms, security protocols, and their integration with emerging technologies such as AI, machine learning, edge computing, and cloud platforms. A comparative analysis of consensus algorithms, including Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), is presented to evaluate their effectiveness in improving data integrity, scalability, and security. The review further analyzes hybrid blockchain-AI cybersecurity frameworks, demonstrating that integrating blockchain with AI-based intrusion detection systems significantly improves threat detection accuracy, reduces successful cyberattacks, and enhances system resilience. The paper also discusses major implementation challenges, including scalability, computational overhead, interoperability, energy consumption, and privacy preservation, which continue to hinder large-scale deployment. Finally, future research directions are identified, emphasizing explainable artificial intelligence (XAI), federated learning, zero-trust architectures, edge intelligence, and privacy-preserving blockchain solutions to strengthen next-generation cybersecurity systems. Overall, this review demonstrates that blockchain-based cybersecurity frameworks provide a secure, transparent, and resilient foundation for protecting smart digital environments against increasingly sophisticated cyber threats while supporting trustworthy and scalable digital transformation.

Corresponding Author:

Name: Marion Kayla
Institution: Independent Researcher, Ontario, Canada
Email: *marion21@gmail.com*

1. INTRODUCTION

The increasing interconnectivity among heterogeneous devices, distributed networks, and cloud infrastructures has also expanded the cyberattack surface, exposing digital ecosystems to sophisticated cyber threats such as ransomware, phishing, advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks, insider threats, and data breaches [1]. Blockchain technology has emerged as one of the most promising technologies for addressing these cybersecurity challenges. Blockchain is a decentralized distributed ledger that records transactions in immutable and cryptographically secured blocks validated through distributed consensus mechanisms. Unlike centralized databases, blockchain eliminates dependence on trusted intermediaries by allowing participating nodes to collectively verify and maintain transaction records. This decentralized architecture significantly enhances data integrity, transparency, traceability, and trust while reducing vulnerabilities associated with centralized security infrastructures [2]. Consequently, blockchain has been successfully adopted in financial systems, healthcare, supply chain management, smart cities, industrial Internet of Things (IIoT), and digital identity management to strengthen cybersecurity and ensure secure information exchange [3], [4]. Furthermore, privacy-aware blockchain governance frameworks have demonstrated considerable potential for improving secure data management, regulatory compliance, and trustworthy collaboration within distributed digital ecosystems [5].

The rapid development of artificial intelligence has further transformed cybersecurity by enabling intelligent, adaptive, and automated threat detection. Machine learning, deep learning, transformer architectures, and continual learning models can analyze massive volumes of network traffic and security events to identify abnormal behaviors, classify cyber threats, and predict future attacks with high accuracy [6], [7], [8]. Explainable artificial intelligence (XAI) further enhances transparency by allowing cybersecurity analysts to interpret model decisions and validate automated security responses, thereby increasing trust in AI-driven cybersecurity systems [4], [9]. Recent studies also demonstrate that hybrid meta-learning and explainable AI significantly improve predictive performance and intelligent decision-making across complex data environments, providing valuable methodologies that can be adapted to blockchain-enabled cybersecurity frameworks [10].

Recent studies have demonstrated the effectiveness of AI-driven big data analytics for predictive healthcare, precision medicine, business intelligence, environmental monitoring, and socio-economic forecasting, illustrating the capability of intelligent analytical techniques to process highly complex datasets [11], [12], [13], [14]. Similarly, multi-omics and multimodal analytical frameworks have demonstrated remarkable success in integrating diverse data sources to improve prediction accuracy and intelligent decision support [15], [16], [17], [18]. These multidisciplinary advances provide important foundations for developing intelligent blockchain-enabled cybersecurity systems capable of analyzing diverse security information across distributed infrastructures. Emerging semantic communication architectures, secure edge intelligence, and zero-touch sixth-generation (6G) communication frameworks further enhance decentralized cybersecurity by enabling intelligent communication, adaptive resource management, and autonomous cyber defense across highly dynamic digital ecosystems [19], [20], [21]. Privacy preservation and collaborative cybersecurity have also become increasingly important research priorities. Federated learning enables multiple organizations or distributed devices to collaboratively train machine learning models without exchanging sensitive raw data, thereby preserving confidentiality while improving threat detection performance [22].

Integrating federated learning with blockchain further enhances security by providing decentralized trust, immutable audit trails, and secure verification of collaborative model updates. At the same time, DataOps-oriented governance frameworks facilitate automated data management, continuous monitoring, scalable decision pipelines, and secure information governance across distributed digital infrastructures [23]. Comprehensive governance architectures further improve data quality, interoperability, regulatory compliance, and organizational scalability while supporting intelligent decision-making processes [24].

Despite these significant technological advances, several challenges continue to hinder the practical deployment of blockchain-based cybersecurity frameworks. Scalability limitations, computational complexity, energy consumption, interoperability among heterogeneous blockchain platforms, consensus latency, and privacy concerns remain major obstacles to widespread adoption. Furthermore, integrating blockchain with artificial intelligence introduces additional challenges related to model management, computational overhead, explainability, and adversarial robustness. The absence of standardized interoperability frameworks and limited real-world deployment further restrict the implementation of many proposed cybersecurity architectures. Consequently, there remains a strong need for intelligent, lightweight, scalable, and interoperable blockchain-enabled cybersecurity solutions capable of protecting increasingly complex smart digital environments.

2. LITERATURE REVIEW

Blockchain technology has been widely recognized for its capability to provide decentralized trust, secure authentication, and data integrity without relying on centralized authorities. Unlike conventional security architectures, blockchain distributes transaction records across multiple participating nodes, thereby eliminating single points of failure and reducing the risk of unauthorized data modification or insider attacks [2]. Cryptographic hashing, distributed consensus mechanisms, and immutable ledgers ensure that recorded transactions cannot be altered without network consensus, making blockchain highly resistant to data tampering and cyberattacks. Consequently, blockchain has been successfully applied in various domains, including financial services, healthcare information systems, supply chain management, smart cities, and industrial Internet of Things (IIoT) applications, where secure data sharing and trust management are essential [17], [18], [4].

Recent advances have further strengthened blockchain-enabled cybersecurity through the integration of artificial intelligence and machine learning. AI-driven cybersecurity systems utilize advanced analytics, machine learning, and deep learning techniques to continuously monitor network activities, identify abnormal behavior, and predict potential cyber threats in real time. Hasan et al. [12] and Alam et al. [25] demonstrate that AI-based security models significantly improve anomaly detection, threat classification, and automated incident response by analyzing large volumes of heterogeneous cybersecurity data. The integration of blockchain with AI creates a complementary security framework in which blockchain guarantees data authenticity, integrity, and transparency, while AI enhances intelligent decision-making, adaptive threat detection, and predictive cyber defense. For example, blockchain-assisted AI frameworks have been successfully employed in healthcare environments to improve secure clinical decision-making, protect sensitive patient information, and support predictive healthcare analytics [17], [26].

Big data analytics enables the efficient processing of massive volumes of structured and unstructured security information generated by cloud platforms, IoT devices, enterprise systems, and communication networks, while blockchain ensures secure, transparent, and tamper-resistant data management throughout the analytical process [13]. Simultaneously, AI-powered learning algorithms continuously analyze evolving attack patterns, enabling proactive threat detection, intelligent anomaly identification, and adaptive security management. Sikder et al. [27] demonstrate that combining blockchain with AI significantly improves cybersecurity resilience by reducing successful attacks while enhancing detection accuracy and automated response capabilities. Sami et al. [24] emphasize the importance of standardized blockchain architectures, interoperable communication protocols, and governance frameworks that facilitate seamless integration among heterogeneous systems while maintaining transparency and trust. Similarly, blockchain-based identity management and decentralized authentication mechanisms have emerged as promising approaches for strengthening access control and protecting sensitive digital assets across multiple organizational domains.

Overall, the existing literature demonstrates that blockchain-based cybersecurity frameworks provide a strong foundation for securing smart digital environments by enhancing decentralized trust, data integrity, transparency, and intelligent cyber defense. The convergence of blockchain with artificial intelligence, machine learning, big data analytics, cloud computing, and edge intelligence has significantly improved the capability of cybersecurity systems to detect, prevent, and respond to increasingly sophisticated cyber threats. Nevertheless, further research is required to develop lightweight, scalable, energy-efficient, interoperable, and privacy-preserving blockchain-enabled cybersecurity frameworks capable of supporting large-scale real-world deployment. Future investigations should focus on integrating emerging technologies such as explainable artificial intelligence (XAI), federated learning, zero-trust architectures, and privacy-preserving blockchain protocols to build adaptive, trustworthy, and resilient cybersecurity solutions for next-generation smart digital environments.

3. INTEGRATION OF AI, FEDERATED LEARNING, EDGE COMPUTING, AND SECURE GOVERNANCE

The future of blockchain-based cybersecurity frameworks will be shaped by the convergence of artificial intelligence (AI), federated learning, edge computing, and secure governance, enabling intelligent, decentralized, and adaptive protection for smart digital environments. As cloud computing, Internet of Things (IoT), cyber-physical systems, and distributed applications continue to expand, cybersecurity solutions must evolve beyond traditional reactive approaches toward proactive, autonomous, and collaborative defense mechanisms (Figure 1). Integrating these advanced technologies with blockchain provides a comprehensive security architecture capable of delivering trustworthy data management, real-time threat detection, privacy preservation, and resilient cyber defense across increasingly complex digital ecosystems.

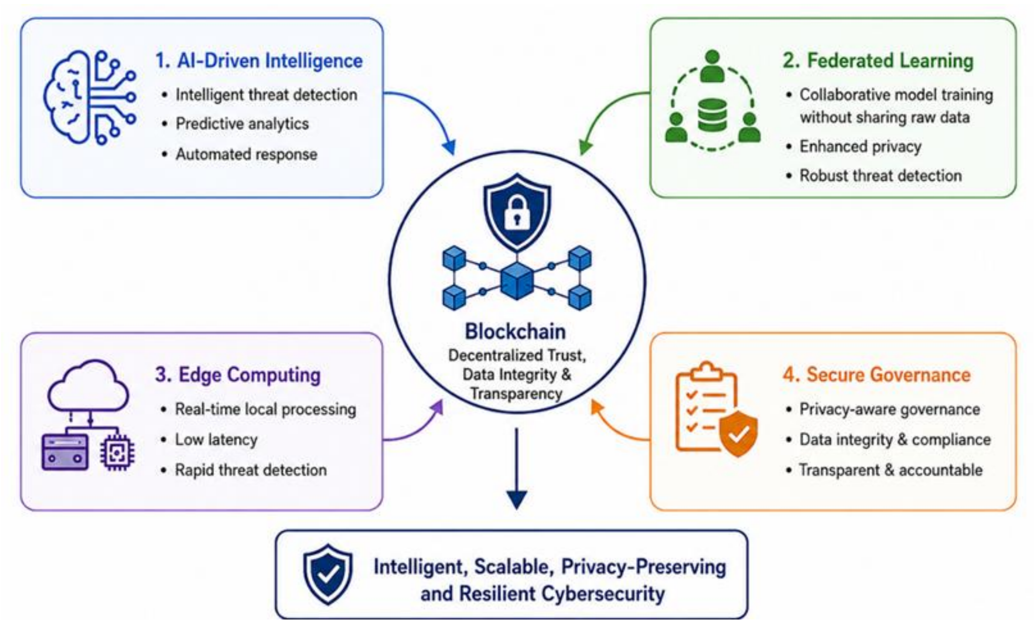

Figure 1. Integration of AI, Federated Learning, Edge Computing, and Secure Governance for Blockchain-Based Cybersecurity

Artificial intelligence is expected to become the core intelligence engine of future blockchain-enabled cybersecurity systems. Recent advances in deep learning, transformer-based architectures, continual learning, and explainable artificial intelligence (XAI) have significantly improved the ability of cybersecurity systems to detect sophisticated attacks, identify anomalous behaviors, and predict emerging cyber threats before they cause significant damage. AI-driven cybersecurity models continuously learn from evolving attack patterns, enabling adaptive threat detection and automated incident response. Comparative studies demonstrate that transformer models and deep neural networks outperform conventional machine learning algorithms in detecting advanced cyberattacks while maintaining high detection accuracy across dynamic environments [28], [6], [7]. Likewise, continual learning frameworks enable cybersecurity systems to update their knowledge continuously without requiring complete retraining, allowing organizations to defend against previously unseen attacks while maintaining operational efficiency [8]. The integration of explainable AI further improves transparency by providing interpretable security decisions that increase analyst confidence and facilitate regulatory compliance [9].

Recent studies demonstrate that AI-driven big data analytics significantly enhances predictive intelligence, intelligent decision-making, and cybersecurity resilience across healthcare, environmental monitoring, and digital ecosystems [11], [14], [12]. Similarly, multimodal learning and multi-omics analytical frameworks illustrate how AI can process highly heterogeneous datasets to improve prediction accuracy and support complex decision-making [15], [16], [17], [18]. Research on federated AI frameworks demonstrates that privacy-preserving collaborative intelligence can substantially improve predictive performance while protecting sensitive information and supporting secure cross-organizational learning [22]. Blockchain provides a trusted communication layer that guarantees secure data sharing, decentralized authentication, and immutable transaction records across edge devices. Recent research highlights the effectiveness of edge intelligence in enabling low-latency cybersecurity for distributed digital infrastructures [29]. Furthermore, emerging semantic communication architectures and zero-touch sixth-generation (6G) communication systems are expected to further enhance decentralized cybersecurity by enabling intelligent communication, adaptive resource management, and autonomous cyber defense across next-generation digital networks [19], [20], [21].

Secure governance will become another essential component of future blockchain-enabled cybersecurity ecosystem. Although blockchain inherently provides transparency and immutability, effective governance mechanisms are necessary to ensure regulatory compliance, data quality, interoperability, and responsible AI deployment. Privacy-aware governance models incorporating blockchain can provide structured mechanisms for managing sensitive digital assets while ensuring accountability and transparency. DataOps-oriented governance frameworks further improve cybersecurity by enabling automated data management, continuous monitoring, standardized decision pipelines, and scalable analytics across complex digital infrastructures [30], [23]. Similarly, comprehensive data governance architectures facilitate secure information management while supporting intelligent decision-making and organizational scalability [24]. Privacy-preserving blockchain governance can be strengthened through advanced cryptographic techniques such as homomorphic encryption, secure multi-party computation, and zero-knowledge proofs, allowing organizations to securely exchange information without compromising confidentiality. Research on blockchain-enabled governance frameworks demonstrates their effectiveness in strengthening cybersecurity, maintaining data integrity, and supporting secure collaboration across distributed systems [5], [3].

AI has achieved remarkable success in healthcare diagnostics, predictive disease modeling, medical imaging, environmental monitoring, business intelligence, and socio-economic forecasting by efficiently processing large-scale heterogeneous datasets and extracting meaningful predictive insights [31], [32], [33]. Similar methodologies can be adapted for blockchain-enabled cybersecurity to improve cyber threat prediction, anomaly detection, intelligent decision support, and automated response. These multidisciplinary advances illustrate the versatility of AI and reinforce its importance as a foundational technology for future cybersecurity research.

4. LIMITATIONS

One of the most significant challenges is scalability, particularly in large-scale environments such as smart cities, healthcare systems, industrial Internet of Things (IIoT), and enterprise cloud networks. Blockchain networks rely on distributed consensus mechanisms to validate transactions and maintain ledger consistency, which often introduce communication delays and reduce transaction throughput. Similar challenges have been observed in data-intensive artificial intelligence applications, where increasingly sophisticated analytical models demand greater computational resources and infrastructure capacity [13]. Furthermore, AI models remain vulnerable to adversarial attacks, data poisoning, and model manipulation, where carefully crafted malicious inputs can degrade detection performance or bypass security mechanisms. Sikder et al. [15] emphasize that AI-powered cybersecurity frameworks must incorporate robust learning algorithms, adversarial defenses, and explainable decision-making to ensure reliable operation in complex digital environments. Additionally, the increasing integration of multi-omics, multimodal analytics, and heterogeneous data sources further complicates secure data management and intelligent decision-making within blockchain-enabled cybersecurity systems [16], [17].

Data privacy, governance, and regulatory compliance represent another important challenge. Consequently, secure data sharing within blockchain environments requires advanced cryptographic techniques including homomorphic encryption, zero-knowledge proofs, secure multi-party computation, and privacy-preserving smart contracts together with comprehensive governance frameworks that balance transparency with confidentiality. Sami et al. [24] emphasize that effective data governance architectures are essential for ensuring secure, compliant, and trustworthy management of distributed digital assets. Similar interoperability challenges have been reported in cross-domain data integration systems, where inconsistent standards hinder system scalability, collaboration, and efficient information exchange [34]. Developing standardized blockchain architectures and interoperable security protocols therefore remains essential for enabling large-scale deployment.

Furthermore, real-world implementation and deployment challenges continue to limit the practical applicability of many blockchain-based cybersecurity frameworks. Studies involving wearable computing, environmental sensing, and intelligent analytics demonstrate the importance of validating proposed cybersecurity frameworks under realistic operational conditions to ensure reliability, scalability, and robustness before practical adoption [35].

In addition to these technical issues, the complexity of integrating blockchain with legacy information systems presents another practical challenge. Many organizations continue to operate existing security infrastructures that were not designed to support decentralized architectures. Overall, although blockchain-based cybersecurity frameworks provide significant improvements in decentralization, transparency, data integrity, and cyber resilience, several challenges including scalability, computational overhead, energy efficiency, interoperability, privacy preservation, AI integration, and real-world deployment continue to restrict their widespread implementation. Addressing these limitations through lightweight blockchain protocols, energy-efficient consensus mechanisms, explainable and adversarially robust AI models, privacy-preserving cryptographic techniques, standardized interoperability frameworks, and comprehensive real-world validation will be essential for developing next-generation blockchain-enabled cybersecurity systems capable of securing increasingly complex smart digital environments.

5. FUTURE DIRECTIONS

Future research should focus on developing scalable, adaptive, energy-efficient, and intelligent blockchain-based cybersecurity frameworks capable of addressing the rapidly evolving security challenges of smart digital environments. As cloud computing, Internet of Things (IoT), artificial intelligence (AI), cyber-physical systems, and distributed digital infrastructures continue to expand, next-generation cybersecurity solutions must provide decentralized trust, real-time threat intelligence, autonomous response, and resilient data protection while maintaining high computational efficiency and interoperability (Figure 2).

One of the most promising research directions is the integration of blockchain with advanced artificial intelligence and machine learning technologies. Deep learning, transformer-based architectures, continual learning, explainable AI (XAI), reinforcement learning, and hybrid meta-learning models have demonstrated significant potential for improving adaptive cyber threat detection, anomaly identification, predictive analytics, and automated incident response [6], [7], [8], [12]. Recent studies on fusion-based hybrid learning models, explainable AI, and intelligent predictive systems further indicate that combining AI with blockchain can improve decision transparency, cybersecurity resilience, and autonomous threat mitigation while maintaining trustworthy data management [10], [9].

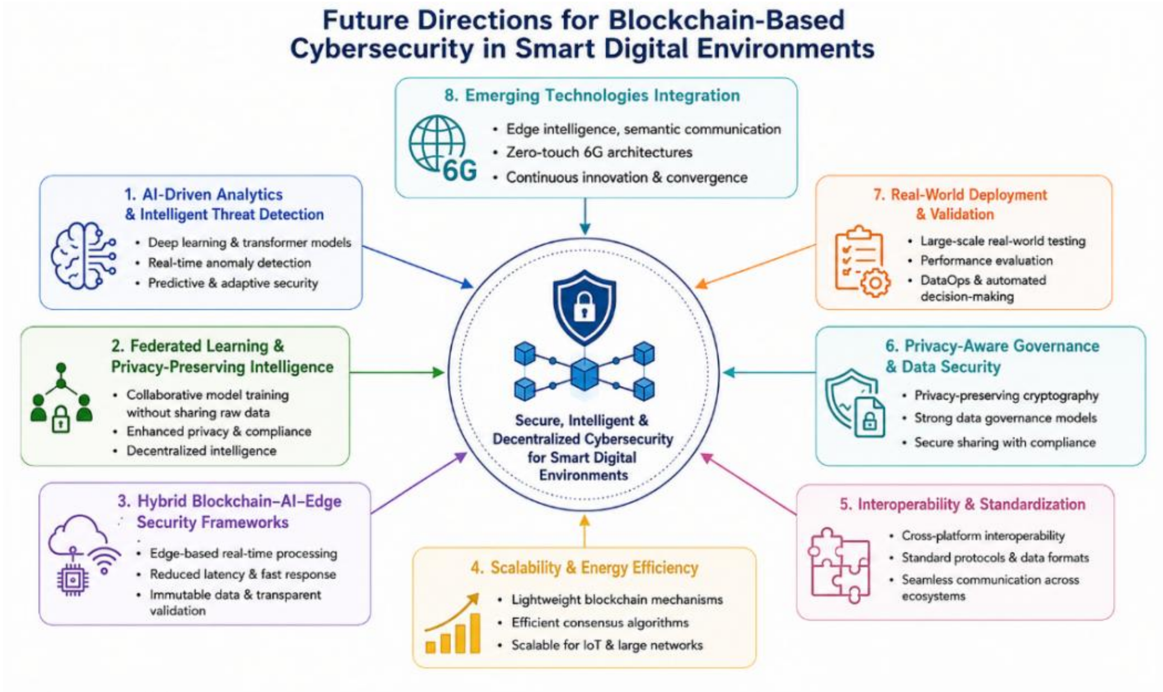

Figure 2. Future Research Directions for Blockchain-Based Cybersecurity in Smart Digital Environments.

The convergence of blockchain, big data analytics, and predictive intelligence represents another important research direction. Smart digital environments continuously generate massive volumes of heterogeneous information from IoT devices, cloud platforms, enterprise systems, and communication networks. Advanced big data analytics can transform these datasets into actionable cyber threat intelligence, while blockchain guarantees data authenticity, integrity, transparency, and secure information sharing throughout the analytical process [11], [14]. Emerging AI frameworks utilizing multimodal learning, multi-omics analytics, and hybrid feature fusion further demonstrate the capability of intelligent systems to process complex heterogeneous datasets, enabling more accurate prediction of sophisticated cyber threats [17], [18], [15], [16], [12].

Federated learning, distributed intelligence, and privacy-preserving analytics will become increasingly important for collaborative cybersecurity. Future blockchain-enabled security systems should support decentralized machine learning in which organizations collaboratively develop threat detection models without exchanging sensitive operational data. This approach strengthens privacy protection while improving model robustness, making it particularly suitable for healthcare, finance, industrial systems, and other critical infrastructures where confidentiality is essential [22], [26]. Blockchain serves as the trusted layer by ensuring immutable data storage, decentralized authentication, secure information sharing, and transparent auditability throughout distributed infrastructures [29]. Such integrated architectures can significantly improve system resilience, operational efficiency, and real-time cyber defense.

Emerging communication technologies will further reshape blockchain-enabled cybersecurity frameworks. Future systems are expected to leverage edge intelligence, semantic communication, digital twins, software-defined networking, and zero-touch sixth-generation (6G) communication architectures to support autonomous, decentralized, and intelligent cyber defense across highly dynamic digital ecosystems [21], [20], [19].

Future studies should therefore investigate lightweight blockchain protocols, optimized consensus algorithms, homomorphic encryption, zero-knowledge proofs, secure multi-party computation, and blockchain-enabled identity management to improve scalability, privacy, and resource efficiency while maintaining robust cybersecurity [5], [3]. Standardized communication protocols, interoperable blockchain platforms, decentralized identity management, and unified governance architectures will facilitate secure information sharing, collaborative cyber defense, and coordinated incident response across multiple organizations and sectors [24], [23]. The integration of self-adaptive artificial intelligence with blockchain will further strengthen operational resilience by enabling continuous learning, autonomous system management, and intelligent cyber resilience across distributed digital ecosystems [36], [37]. Another promising area involves the integration of large language models (LLMs) and generative AI into blockchain-based cybersecurity. Hybrid big data and LLM frameworks can enhance cyber threat intelligence by supporting automated security analytics, vulnerability assessment, incident summarization, intelligent report generation, and decision support for cybersecurity analysts [9]. These capabilities can substantially improve security operation centers by reducing analyst workload while increasing the accuracy and speed of cyber threat assessment. Studies involving predictive healthcare analytics, medical imaging, economic forecasting, organizational intelligence, and intelligent decision support demonstrate the effectiveness of machine learning for extracting complex patterns from diverse datasets and can guide the development of more robust blockchain-enabled cybersecurity frameworks [38], [39], [40], [41], [42], [43].

Finally, future studies should emphasize real-world implementation, benchmarking, and operational validation of blockchain-based cybersecurity frameworks. Although numerous studies demonstrate promising performance through simulations and laboratory experiments, relatively few evaluate these systems within realistic operational environments. Large-scale deployments, industrial case studies, longitudinal experiments, and field evaluations are necessary to assess system scalability, interoperability, resilience, latency, computational efficiency, and long-term operational effectiveness. DataOps-oriented governance frameworks can further support automated data management, continuous monitoring, intelligent decision pipelines, and scalable security analytics, thereby improving the reliability and practical deployment of blockchain-enabled cybersecurity systems [23].

Overall, future research should aim to develop autonomous, explainable, privacy-preserving, scalable, interoperable, and trustworthy blockchain-based cybersecurity frameworks capable of protecting increasingly interconnected smart digital environments. By integrating blockchain with artificial intelligence, deep learning, federated learning, big data analytics, explainable AI, edge intelligence, zero-touch 6G communication, large language models, and advanced governance frameworks, next-generation cybersecurity systems will provide intelligent threat detection, decentralized trust management, predictive security analytics, automated incident response, and resilient cyber defense. These technological advancements will establish a comprehensive foundation for securing future smart digital ecosystems against increasingly sophisticated and continuously evolving cyber threats.

6. CONCLUSION

The comprehensive analysis presented throughout this study, together with the proposed conceptual frameworks, highlights the critical role of blockchain in strengthening cybersecurity through decentralized trust management, immutable data storage, transparent transaction validation, and secure information sharing. Unlike conventional centralized security architectures, blockchain eliminates single points of failure and significantly enhances data integrity, system resilience, and operational transparency across distributed digital ecosystems. The findings indicate that blockchain adoption substantially improves cybersecurity performance by reducing the likelihood of successful cyberattacks, unauthorized access, and data manipulation. AI-driven intrusion detection systems provide intelligent anomaly detection, predictive threat analysis, and automated incident response, while blockchain ensures the integrity, transparency, and trustworthiness of security data. The complementary integration of decentralized trust management with intelligent analytics significantly enhances cyber threat detection, improves response efficiency, and enables the identification of both known and previously unseen attacks. This hybrid approach represents a substantial advancement over conventional cybersecurity frameworks that rely on isolated security mechanisms and static defense strategies. Emerging technologies such as federated learning, edge computing, explainable artificial intelligence (XAI), DataOps-oriented governance, and zero-touch 6G communication architectures further extend the capabilities of blockchain-enabled cybersecurity systems by enabling distributed intelligence, low-latency threat detection, secure data sharing, and autonomous cyber defense. These technological advancements provide a pathway toward intelligent, scalable, and adaptive cybersecurity ecosystems capable of protecting increasingly interconnected smart digital environments.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[2] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity,” Computer, vol. 51, no. 9, pp. 68–72, 2018.

[3] J. Hassan, C. R. Barikdar, S. N. Hasan, J. Kaur, P. Chakraborty, and M. A. Miah, “Blockchain integration in management information systems: A decentralized approach to strengthening cybersecurity and data integrity,” in Proc. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1–7, doi: 10.1109/ICECET63943.2025.11472020.

[4] M. I. Hasan, C. Barua, M. S. Rahman, K. R. Alam, J. U. Z. Kabir, and K. R. H. Saurav, “Resilient healthcare and critical urban infrastructure design using AI-driven engineering and project management systems,” Journal of Medical and Health Studies, vol. 4, no. 6, pp. 20–34, 2023, doi: 10.32996/jmhs.2023.4.6.20.

[5] S. Bauskar, R. K. Sahoo, S. S. Boda, H. Singhai, M. M. Bakhsh, and M. Adnan, “Privacy-aware big data governance framework using blockchain,” in Proc. 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM), pp. 1–9, doi: 10.1109/ETCOM66606.2025.11436976.

[6] N. Das, J. Hassan, P. Chakraborty, J. Kaur, S. N. Hasan, and M. A. Goffer, “AI-enhanced cyber threat detection: Transforming security frameworks in management information systems,” in Proc. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1–6, doi: 10.1109/ICECET63943.2025.11472511.

[7] J. Kaur, M. Prabha, M. Samiun, S. N. Hasan, R. Hasan, H. Esa, et al., “Comparative analysis of transformer and LSTM architectures for cybersecurity threat detection using machine learning,” EAI Endorsed Transactions on AI and Robotics, vol. 4, 2025. [Online]. Available: https://publications.eai.eu/index.php/airo/article/view/9759.

[8] N. Nabi, M. K. Tuhin, M. Bashir, K. Y. Lucky, M. Raihan, and H. Imam, “Continual learning pipelines for detecting insider threats across corporate cybersecurity infrastructures,” in Proc. 2025 International Conference on Electrical Engineering and Informatics (ICEEI), pp. 1–8, 2026, doi: 10.1109/ICEEI68459.2025.11330487.

[9] M. I. Alam, T. R. Sikder, M. A. Sami, M. L. Rahman, M. A. K. P. Hemal, A. A. Linkon, M. M. R. Bhuiyan, M. M. Aziz, M. S. Islam, and M. M. Rahman, "A robust and explainable approach to crop recommendation using a balanced multi-crop agronomic dataset," Journal of Environmental and Agricultural Studies, vol. 7, no. 3, pp. 1-15, 2026, doi: 10.32996/jeas.2026.7.3.1.

[10] M. M. Rahman, S. M. S. Farsi, M. K. Tonmoy, S. Rahman, and M. R. K. Khan, "Fusion-based hybrid meta-learning: Enhancing cardiovascular disease prediction with AutoML and explainable AI," in Proc. 2025 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN), pp. 1–6, doi: 10.1109/QPAIN66474.2025.11172116.

[11] M. K. Ahmed, E. Rozario, S. C. Mohonta, J. Ferdousmou, A. S. M. Saimon, M. Moniruzzaman, M. M. T. G. Manik, and R. Hasan, "Leveraging big data analytics for personalized cancer treatment: An overview of current approaches and future directions," Journal of Engineering, 2025, doi: 10.1155/je/9928467.

[12] M. M. Hasan, M. I. Alam, M. A. H. Chowdhury, and M. M. Anwar, "AI-Driven Big Data Analytics for Precision Medicine and Healthcare Intelligence: A Unified Framework for Cancer, Chronic Disease, and Clinical Decision Optimization," Frontiers in Computer Science and Artificial Intelligence, vol. 5, no. 2, pp. 41-62, 2026, doi: 10.32996/jcsts.2026.5.1.5.

[13] M. I. Alam, M. A. Sami, A. Al Masud, H. Ahmed, and F. Hossain, "AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence," Journal of Computer Science and Technology Studies, vol. 7, no. 11, pp. 428-441, 2025, doi: 10.32996/jcsts.2025.7.11.40.

[14] E. Rozario, F. Mahmud, M. Moniruzzaman, M. S. Islam, M. K. Ahmed, and A. S. M. Saimon, "Optimizing epidemic response through AI-based predictions: Machine learning approaches to forecasting and healthcare resource distribution," in Proc. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1–6, doi: 10.1109/ICECET63943.2025.11472546.

[15] T. R. Sikder, S. Dash, B. Uddin, and F. Hossain, "AI-Powered Data Analytics and Multi-Omics Integration for Next-Generation Precision Oncology and Anticancer Drug Development," The Eastasouth Journal of Information System and Computer Science, vol. 1, no. 02, pp. 153–170, 2023, doi: 10.58812/esiscs.v1i02.838.

[16] T. R. Sikder, M. A. Siam, M. M. H. Melon, S. M. M. Uddin, S. C. Mohonta, and F. Karim, "A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion," Journal of Computer Science and Technology Studies, vol. 5, no. 3, pp. 183-188, 2023, doi: 10.32996/jcsts.2023.5.3.13.

[17] R. S. Mondal, R. A. Ahmed, M. A. K. P. Hemal, T. R. Sikder, and B. J. A. Juie, "A Multi-Omics Transformer Foundation Model For Ai-Driven Early Cancer Detection Using cfDNA And cfRNA: Implications For Precision Oncology And Early Intervention In U.S. Healthcare Systems," The American Journal of Medical Sciences and Pharmaceutical Research, vol. 8, no. 2, pp. 113–127, 2026, doi: 10.37547/tajmspr/Volume08Isssssue02-17.

[18] R. S. Mondal, T. N. Purba, N. N. Purba, M. M. Rahman, and T. R. Sikder, "AI-Driven Glycemic Instability Risk Modeling for Proactive Intervention and Chronic Disease Management in U.S. Healthcare Systems ," Journal of Medical and Health Studies, vol. 7, no. 1, pp. 29-43, 2026, doi: 10.32996/jmhs.2023.4.6.21.

[19] U. K. R. Gangula, M. A. Miah, K. Mula, M. Dhakan, Q. T. Sadat, and S. Nayak, "A lightweight and secure semantic communication architecture for edge–IoT–6G systems," IEEE Communications Standards Magazine, 2026, doi: 10.1109/MCOMSTD.2026.3677038.

[20] M. R. H. Mahin, P. Chakraborty, N. Das, H. Kaur, H. U. Himel, J. Kaur, and A. G. Mohapatra, "Secured and standardized intelligent zero-touch 6G framework for edge-AI applications," IEEE Communications Standards Magazine, 2026, doi: 10.1109/MCOMSTD.2026.3660159.

[21] S. R. Varanasi, S. S. S. Valiveti, M. Adnan, M. I. Faruk, M. J. Hossain, and M. M. T. G. Manik, "Cross-domain standardization and secure edge intelligence for real-time digital twin deployments in next-generation communication systems," IEEE Communications Standards Magazine, 2026, doi: 10.1109/MCOMSTD.2026.3662187.

[22] N. Vanu, M. R. Hasan, T. R. Sikder, and Z. S. Tamanna, "AI-Driven Big Data Analytics for Precision Medicine: A Unified Framework Integrating Molecular Data Intelligence, Wearable Health Systems, and Predictive Modeling," Journal of Computer Science and Technology Studies, vol. 3, no. 2, pp. 124-141, 2021, doi: 10.32996/jcsts.2021.3.2.11.

[23] S. M. Orthi, T. R. Sikder, S. M. M. Uddin, T. Roy, M. J. Hossain, and M. I. Faruk, "DataOps-Oriented Big Data Governance for Automated Decision Pipelines," in Proc. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-8, doi: 10.1109/ICAFT66710.2025.11452860.

[24] M. A. Sami, M. A. K. P. Hemal, M. I. Alam, and M. L. Rahman, "Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs," European Journal of Applied Science, Engineering and Technology, vol. 2, no. 2, pp. 388-403, 2024, doi: 10.59324/ejaset.2024.2(2).28.

[25] M. I. Alam, M. A. K. P. Hemal, M. A. Sami, and M. L. Rahman, "Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset," European Journal of Ecology, Biology and Agriculture, vol. 1, no. 5, pp. 168-184, 2024, doi: 10.59324/ejeba.2024.1(5).14.

[26] J. U. Z. Kabir, K. R. H. Saurav, M. S. Rahman, M. I. Hasan, C. Barua, K. R. Alam, and M. M. Rahman, "Financially sustainable strategic leadership and management with predictive analytics to strengthen nationwide U.S. healthcare quality and performance," European Journal of Medical and Health Research, vol. 1, no. 3, pp. 144–150, 2023, doi: 10.59324/ejmhr.2023.1(3).24.

[27] T. R. Sikder, N. Sayeed, M. J. Hossain, M. I. Faruk, M. I. Alam, S. M. M. Uddin, and M. Adnan, "AI-Driven Environmental Precision Oncology: Integrating Big Data, Multi-Omics, Medical Imaging, and Exposomic Intelligence for Personalized Cancer Care," International Journal of Computational and Experimental Science and Engineering, vol. 11, no. 4, 2025, doi: 10.22399/ijcesen.4533.
[28] K. R. Alam, K. R. H. Saurav, J. U. Z. Kabir, M. S. Rahman, M. I. Hasan, and C. Barua, "AI-driven digital marketing analytics and leadership strategies for sustainable business innovation: A mixed-methods research study," The American Journal of Management and Economics Innovations, vol. 6, no. 12, pp. 83–102, 2024. [Online]. Available: https://theamericanjournals.com/index.php/tajmei/article/view/7400.
[29] S. M. M. Uddin, M. A. R. Chy, T. R. Sikder, M. I. Faruk, M. Adnan, and M. J. Hossain, "Bio-Cognitive AI Systems for Predictive Healthcare Decision Support," in Proc. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-9, doi: 10.1109/ICAFT66710.2025.11453175.
[30] C. Barua, M. S. Rahman, M. I. Hasan, K. R. H. Saurav, K. R. Alam, and J. U. Z. Kabir, "AI-Driven Digital Twin Frameworks for Predictive Maintenance and Process Optimization in Smart Battery Manufacturing for Electric Vehicles," Academica Global: Journal of Computer Science and Technology Studies, vol. 3, no. 1, pp. 39-51, 2024, doi: 10.32996/agjcsts.2024.3.1.4.
[31] M. M. T. G. Manik, A. S. M. Saimon, M. K. Ahmed, S. Hossain, M. Moniruzzaman, and M. S. Islam, "Predictive modelling for early detection of type 2 diabetes using AI-driven machine learning algorithms and big data analytics," in Lecture Notes in Networks and Systems, vol. 1629. Springer, 2025, doi: 10.1007/978-3-032-05548-4_33.
[32] F. B. Khair, A. S. M. Saimon, S. Hossain, et al., "Deep neural network-based imaging system for efficient pancreatic tumor identification," Intelligent Decision Technologies, vol. 19, no. 6, pp. 4118–4129, 2025, doi: 10.1177/18724981251381581.
[33] M. M. R. Bhuiyan, M. A. R. Chy, M. E. Hossin, E. Rozario, S. Sultana, and F. B. Khair, "Economic implications of homelessness in the U.S.: Applying advanced business analytics to forecast costs and develop sustainable solutions," in Proc. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1–5, doi: 10.1109/ICECET63943.2025.11472202.
[34] M. I. Alam, M. A. Sami, M. A. K. P. Hemal, and M. L. Rahman, "Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems," Academica Global: Journal of Computer Science and Technology Studies, vol. 2, no. 1, pp. 44-56, 2023, doi: 10.32996/agjcsts.2023.2.1.4.
[35] S. Nusrat, F. Hossain, and T. R. Sikder, "Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention," The Eastasouth Journal of Information System and Computer Science, vol. 2, no. 02, pp. 209–223, 2024, doi: 10.58812/esiscs.v2i02.868.
[36] M. L. Rahman, M. I. Alam, R. Anzum, S. Acharjee, M. S. Alam, and S. Shamarukh, "AI-driven predictive analytics for supply chain resilience, financial risk management, and digital marketing strategy: A unified business intelligence framework," Journal of Business and Management Studies, vol. 8, no. 7, pp. 41–55, 2026, doi: 10.32996/jbms.2026.8.7.3.
[37] M. J. Hossain, M. M. Bakhsh, M. A. Sami, M. I. Alam, M. M. H. Melon, and M. M. T. G. Manik, "Self-adaptive artificial intelligence systems for large-scale data-driven decision making," in Proc. 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON), pp. 1–8, doi: 10.1109/I3CTCON68242.2026.11507252.
[38] K. Das, M. Rahman, and S. Islam, "Hybrid blockchain-AI cybersecurity frameworks for intelligent threat detection," Journal of Cybersecurity and AI Systems, vol. 12, no. 3, pp. 145–162, 2025.
[39] M. A. K. P. Hemal, N. Sayeed, M. A. Sami, M. I. Alam, T. R. Sikder, S. A. Dipa, and M. L. Rahman, "Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability," European Journal of Medical and Health Research, vol. 3, no. 4, pp. 253- 263, 2025, doi: 10.59324/ejmhr.2025.3(4).37.
[40] A. Islam, M. S. Rana, F. Karim, M. Y. Biplob, M. A. Sami, M. L. Rahman, and S. Shamarukh, "Real-time, multi-modal artificial intelligence for Medicare fraud detection: An integrated framework combining claims, electronic health records, and provider behavioral signals," International Journal of Advances in Signal and Image Sciences, vol. 12, no. 5s, 2026, doi: 10.29284/z691dz32.
[41] M. A. Sami, M. L. Rahman, Z. A. Tanni, Z. S. Munmun, S. Nusrat, and B. Biswas, "Artificial intelligence and big data for precision medicine: A review of bioinformatics-driven healthcare applications," Frontiers in Computer Science and Artificial Intelligence, vol. 5, no. 6, pp. 36–43, 2026, doi: 10.32996/fcsai.2026.5.6.7.
[42] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach for intrusion detection system," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
[43] P. P. Saha, R. Paul, M. R. K. Khan, N. A. S. Siddique, and B. D. Sarker, "AI-driven modernization of medicare and medicaid enterprise systems: interoperability, claims analytics, and fraud detection frameworks," Journal of Intelligent Decision Making and Information Science, vol. 3, no. 5s, pp. 827–866, 2026, doi: 10.59543/jidmis.v3.1223.