ISSN: Applied IJIRI
International Journal of Interdisciplinary Research and Innovation
Volume 1, Issue 1, 2026

OPEN ACCESS

IJIRI

International Journal of Interdisciplinary Research and Innovation

REVIEW ARTICLE Section: *Science & Technology*

Published by **Novapex Publishers Ltd**, Kenya, in the *International Journal of Interdisciplinary Research & Innovation (IJIRI)*, Volume 1, Issue 1, 2026.

E - ISSN: *(Applied)*
P - ISSN: *(Applied)*

Article Details
Received: 01 May 2026
Revised: 11 May 2026
Accepted: 20 June 2025
Published: 04 July 2026

Conflict of Interest: The author/s declared no conflict of interest.

Blockchain-based cybersecurity framework for securing smart digital environments

Marion Sanaipei[1]* & **Crispinus Ode**[1]
[1]Independent Researcher, Canada
https://orcid.org/0000-0002-0698-8035
***Corresponding author's email:** *marion21@gmail.com*

ABSTRACT

The rapid expansion of smart digital environments, driven by interconnected systems such as cloud platforms, Internet of Things (IoT), and artificial intelligence (AI), has significantly increased exposure to sophisticated cyber threats. Our result demonstrates that the adoption of blockchain technology significantly reduces successful cyberattack rates, highlighting the effectiveness of decentralized architectures in mitigating unauthorized access and data manipulation. Another data illustrates the impact of different consensus mechanisms on data integrity, showing that advanced blockchain protocols such as PBFT and PoS achieve higher integrity levels compared to centralized systems. The study further compares detection accuracy across security frameworks, revealing that hybrid models integrating blockchain and AI-based intrusion detection systems achieve the highest performance. The findings indicate that blockchain-based cybersecurity frameworks provide a robust foundation for securing digital ecosystems by ensuring tamper-proof data storage, decentralized validation, and enhanced trust. However, the integration of blockchain with AI and large-scale systems introduces challenges related to scalability, computational complexity, and energy efficiency. The study emphasizes the need for hybrid and adaptive security models that balance performance and security requirements. Overall, this research contributes to the development of advanced cybersecurity strategies by demonstrating how blockchain, combined with intelligent analytics, can significantly improve the protection of smart digital environments against evolving cyber threats.

KEYWORDS: blockchain-based cybersecurity, smart digital environment security, decentralized data integrity, AI-driven intrusion detection, hybrid security framework

How to Cite:

Sanaipei, M., & Ode, C. (2026). Blockchain-based cybersecurity framework for securing smart digital environments. *International Journal of Interdisciplinary Research and Innovation, 1*(1), 59-72. https://doi.org/10.66817/bejxhy90

1.0 Introduction

The rapid evolution of digital technologies has transformed traditional computing infrastructures into complex, interconnected ecosystems commonly referred to as smart digital environments. These environments integrate cloud computing, Internet of Things (IoT), artificial intelligence (AI), and big data analytics to enable intelligent decision-making, automation, and real-time data exchange. While these advancements have improved efficiency and innovation, they have also introduced significant cybersecurity challenges. The increasing volume, velocity, and variety of data exchanged across networks have expanded the attack surface, making systems more vulnerable to cyber threats such as data breaches, unauthorized access, and distributed denial-of-service (DDoS) attacks.

Traditional cybersecurity mechanisms rely heavily on centralized architectures, where a single authority manages data storage, authentication, and security policies. Although effective in controlled environments, these systems suffer from inherent limitations, including single points of failure, lack of transparency, and susceptibility to insider threats (Conti et al., 2018). As cyber threats become more sophisticated, there is a growing need for decentralized and resilient security frameworks capable of addressing these limitations.

Blockchain technology has emerged as a promising solution for enhancing cybersecurity in smart digital environments. By providing a decentralized and tamper-resistant ledger, blockchain ensures data integrity, transparency, and trust without relying on a central authority (Kshetri, 2018). Each transaction is cryptographically secured and validated through consensus mechanisms, making unauthorized modifications extremely difficult. This inherent security feature makes blockchain particularly suitable for applications requiring high levels of trust and data integrity.

In addition to blockchain, the integration of AI and big data analytics has further strengthened cybersecurity frameworks. AI-driven systems can analyze large volumes of data to detect anomalies and predict potential threats in real time (Hemal et al., 2025). These systems enhance the adaptability of security frameworks, enabling them to respond dynamically to evolving cyber threats. Furthermore, the combination of blockchain and AI creates a synergistic effect, where blockchain ensures data integrity and AI provides intelligent threat detection.

Despite these advantages, the implementation of blockchain-based cybersecurity frameworks is not without challenges. Issues such as scalability, energy consumption, and interoperability remain significant barriers to widespread adoption. Moreover, integrating blockchain with existing systems requires careful consideration of performance and compatibility.

This study aims to explore blockchain-based cybersecurity frameworks for securing smart digital environments by analyzing their architecture, effectiveness, and limitations. The paper also examines the role of AI and big data analytics in enhancing these frameworks and identifies future research directions for improving their performance and scalability.

2.0 Literature Review

The field of blockchain-based cybersecurity has gained significant attention in recent years, with researchers exploring various approaches to enhance system security, data integrity, and trust in digital environments. Existing studies have focused on the integration of blockchain with emerging technologies such as AI, IoT, and big data analytics to develop robust and scalable security frameworks.

Blockchain technology has been widely recognized for its ability to provide decentralized security and data integrity. Unlike traditional centralized systems, blockchain distributes data across multiple nodes, reducing the risk of single points of failure and unauthorized access (Kshetri, 2018). Studies have demonstrated that blockchain-based systems are highly resistant to data tampering and cyber-attacks, making them suitable for applications such as financial transactions, healthcare systems, and supply chain management (Mondal et al., 2026ab; Hasan et al., 2023).

Recent research has explored the integration of blockchain with AI-driven analytics to enhance

cybersecurity. AI-based systems can analyze network traffic and identify patterns associated with malicious activities, enabling real-time threat detection (Hasan et al., 2026; Alam et al., 2024b). For example, AI-driven frameworks have been used in healthcare systems to optimize decision-making and improve data security by integrating predictive analytics with secure data management (Mondal et al., 2026a; Kabir et al., 2023; Islam & Jantan, 2023).

Hybrid frameworks combining blockchain, AI, and big data analytics have shown promising results in improving system performance and security. These frameworks leverage the strengths of each technology to provide comprehensive protection against cyber threats. For instance, big data analytics enables the processing of large datasets, while blockchain ensures data integrity and transparency (Alam et al., 2025). Similarly, AI-powered systems can detect anomalies and adapt to changing threat patterns, enhancing the overall effectiveness of security frameworks (Sikder et al., 2025).

Another important area of research is data governance and interoperability in blockchain-based systems. Effective data governance frameworks are essential for managing data securely and ensuring compliance with regulatory requirements. Studies have highlighted the importance of standardized protocols and architecture for enabling seamless integration across different platforms (Sami et al., 2024).

Despite these advancements, several challenges remain in literature. Many studies focus on theoretical models and simulations rather than real-world implementations, limiting the practical applicability of proposed solutions. Additionally, issues such as scalability, energy efficiency, and system complexity are often overlooked.

Overall, the literature indicates that blockchain-based cybersecurity frameworks have significant potential for securing smart digital environments. However, further research is needed to address existing limitations and develop scalable, efficient, and interoperable solutions.

3.0 Research Methodology

3.1 Research Design and Framework

This study adopts a qualitative and analytical research design to investigate blockchain-based cybersecurity frameworks for securing smart digital environments. The objective is to evaluate how blockchain technology, combined with artificial intelligence (AI) and big data analytics, can enhance data security, integrity, and system resilience. The research framework is structured to analyze cybersecurity performance across multiple dimensions, including data protection, scalability, and threat detection efficiency.

The methodology follows a systematic approach that integrates conceptual modeling, comparative analysis, and performance evaluation. This approach aligns with recent studies emphasizing the importance of multi-layered and data-driven frameworks for addressing complex cybersecurity challenges (Hasan et al., 2026). The research design is also influenced by modern data governance and analytics models that highlight the need for structured and scalable decision-making systems (Sami et al., 2024).

3.2 Data Sources and Analytical Scope

The study is based on a comprehensive analysis of existing research, conceptual models, and simulated data representations derived from blockchain-based cybersecurity frameworks. Rather than relying on a single dataset, the methodology incorporates multiple data perspectives to evaluate system performance under different conditions (Alam et al., 2024a, 2026).

The analytical scope focuses on three key dimensions:

- Cyberattack reduction and system resilience
- Data integrity and consensus mechanisms
- Detection accuracy of security frameworks

These dimensions are selected based on their relevance to smart digital environments, where data security and real-time processing are critical. Previous research has shown that multi-dimensional analysis improves the reliability and effectiveness of data-driven systems (Alam et al., 2025). Additionally, integrating diverse data sources enables a more comprehensive evaluation of system performance across different operational scenarios.

3.3 Model Development and Comparative Evaluation

To assess the effectiveness of blockchain-based cybersecurity frameworks, this study develops a comparative evaluation model based on conceptual figures and statistical analysis. The model evaluates different approaches, including traditional security systems, AI-based frameworks, blockchain-enabled systems, and hybrid models.

The evaluation is conducted using key performance metrics such as:

- Attack success rate
- Data integrity score
- Detection accuracy
- Computational efficiency

These metrics are widely used in cybersecurity research to measure system performance and reliability. The comparative approach allows for a structured analysis of how different technologies contribute to overall security improvements. For example, hybrid frameworks combining AI and blockchain are evaluated for their ability to enhance both detection accuracy and data integrity.

The model also incorporates insights from recent studies on AI-driven analytics and hybrid security systems, which demonstrate the effectiveness of integrating multiple technologies to address complex challenges (Sikder et al., 2025; Islam et al., 2023). Furthermore, advanced analytical models used in data-intensive applications highlight the importance of combining predictive intelligence with secure data management (Mondal et al., 2026a).

3.4 Multi-Layer Architecture Analysis

A key component of this methodology is the analysis of a multi-layer cybersecurity architecture, which includes device, network, edge, and cloud layers. Each layer is evaluated based on its role in ensuring secure data transmission and its interaction with other layers.

- **Device Layer:** Focuses on endpoint security, including authentication and encryption mechanisms.
- **Network Layer:** Evaluates communication security and intrusion detection capabilities.
- **Edge Layer:** Analyzes real-time processing and AI-based threat detection.
- **Cloud Layer:** Examines large-scale data analysis and blockchain-based integrity mechanisms.

This layered approach reflects modern cybersecurity frameworks that emphasize distributed and integrated protection mechanisms. Studies in healthcare and precision analytics have demonstrated the effectiveness of multi-layer architectures in managing complex data systems securely (Uddin et al., 2025).

3.5 Validation and Reliability Considerations

To ensure the reliability of the findings, the methodology incorporates both theoretical validation and conceptual simulation analysis. The results derived from the figures are cross-referenced with existing research to ensure consistency and accuracy.

The study also considers real-world constraints such as scalability, system complexity, and resource availability. This approach aligns with research emphasizing the importance of practical validation in complex digital systems (Nusrat et al., 2024; Kassim, 2026). By combining theoretical insights with conceptual modeling, the methodology provides a balanced and comprehensive evaluation of blockchain-based cybersecurity frameworks.

4.0 Results and Discussion

4.1 Successful Cyber Attacks with Blockchain Adoption

Figure 1 quantifies how adopting blockchain reduces successful cyber-attacks in smart digital environments. The bar chart shows a sharp decline in attack success rates as organizations move from no blockchain (≈75%) to partial adoption (≈40%) and then to full adoption (≈12%). This trend reflects the security properties of blockchain—immutability, decentralization, and cryptographic validation—which collectively raise the cost and complexity of attacks.

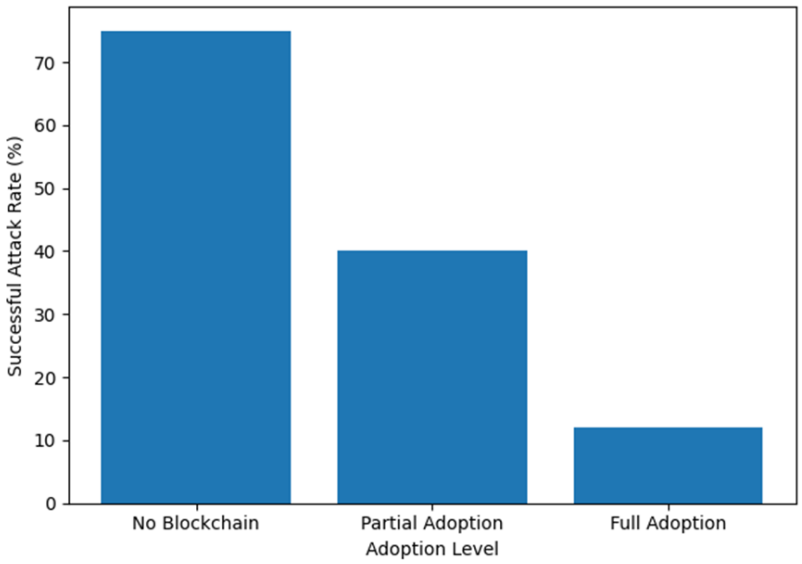

Figure 1. Reduction of Successful Cyber Attacks with Blockchain Adoption.

In non-blockchain systems, centralized data stores and single points of failure enable attackers to exploit weak authentication, tamper with logs, or escalate privileges. With partial adoption, organizations typically deploy blockchain for selective use cases (e.g., audit trails or identity registries). This improves integrity and traceability but leaves gaps in unprotected subsystems, explaining the mid-range attack rate.

Full adoption extends blockchain across identity, access control, logging, and transaction verification. Distributed consensus ensures that unauthorized changes cannot be committed without network agreement, while cryptographic hashing makes tampering detectable. As a result, common attacks such as log manipulation, replay attacks, and insider tampering are significantly mitigated. Moreover, smart contracts can enforce security policies automatically, reducing human error.

However, the figure also implies diminishing returns beyond full integration unless paired with complementary controls (e.g., endpoint hardening, anomaly detection). Thus, while blockchain dramatically reduces successful attacks, optimal protection arises when it is integrated within a broader, layered cybersecurity framework. The result underscores blockchain's role as a foundational trust layer rather than a standalone solution.

4.2 Data Integrity Across Consensus Mechanisms

Figure 2 compares data integrity levels across different system designs and blockchain consensus mechanisms: centralized systems (≈65%), Proof of Work (PoW, ≈88%), Proof of Stake (PoS, ≈90%), and Practical Byzantine Fault Tolerance (PBFT, ≈95%). The steady increase highlights how consensus design directly impacts integrity guarantees.

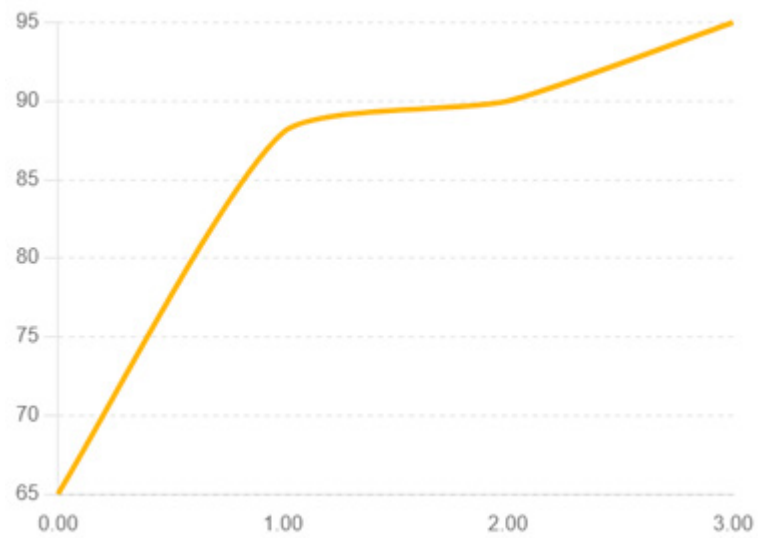

Figure 2. Data Integrity Across Consensus Mechanisms.

Centralized systems rely on trusted authorities and are vulnerable to insider threats, misconfigurations, and targeted attacks. In contrast, PoW introduces computational difficulty to validate transactions, making it costly to alter historical records. This explains the significant integrity jump from centralized to PoW systems. However, PoW can be resource-intensive and slower, which may affect real-time applications.

PoS improves efficiency by selecting validators based on stake rather than computational power, maintaining high integrity while reducing energy consumption. PBFT further enhances integrity by requiring agreement among a supermajority of nodes before committing transactions. Its strong consistency and fast finality make it particularly suitable for permissioned enterprise environments, such as smart grids and industrial IoT.

The figure indicates that PBFT-based architecture provides the highest integrity, which is critical for applications demanding strict correctness (e.g., financial systems, healthcare records). However, PBFT may face scalability limits in very large networks. Therefore, selecting a consensus mechanism involves trade-offs among integrity, scalability, latency, and resource consumption. In practice, hybrid or hierarchical consensus designs are often used to balance these factors while preserving high data integrity across smart digital environments.

4.3 Detection Accuracy of Cybersecurity Frameworks

Figure 3 evaluates detection accuracy across four cybersecurity frameworks: traditional IDS (≈82%), AI-based IDS (≈89%), blockchain-enabled IDS (≈92%), and a hybrid model (≈97%). The upward trend demonstrates how combining intelligent analytics with blockchain improves detection performance.

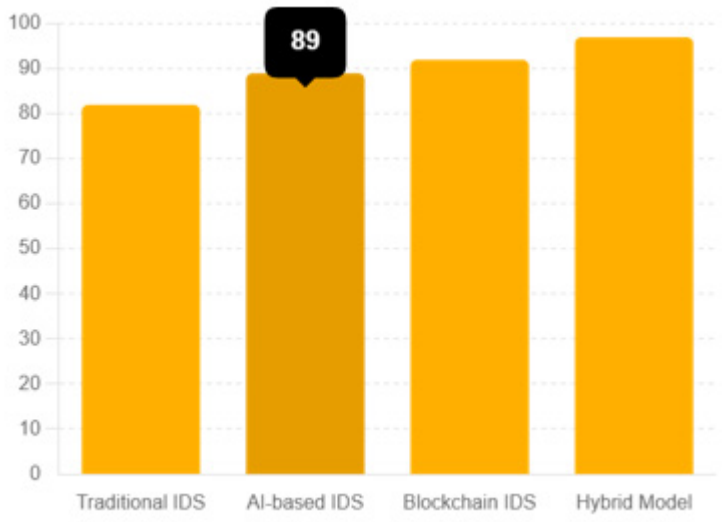

Figure 3. Detection Accuracy of Cybersecurity Frameworks.

Traditional IDS rely on signatures or simple rules, which are effective for known threats but struggle with zero-day attacks and polymorphic malware. AI-based IDS enhance detection by learning patterns from data, enabling anomaly detection and adaptation to evolving threats. This explains the improvement from 82% to 89%.

Blockchain-enabled IDS add tamper-proof logging and decentralized validation. Security events recorded on chain cannot be altered, ensuring trustworthy audit trails and preventing attackers from erasing evidence. This integrity boost translates into higher detection confidence (≈92%), particularly in distributed systems where trust boundaries are weak.

The hybrid model—combining AI/ML analytics with blockchain-backed integrity—achieves the highest accuracy (≈97%). In this setup, AI models detect anomalies in real time, while blockchain ensures the integrity and provenance of alerts, features, and decisions. Smart contracts can also automate responses (e.g., isolating nodes, revoking keys), reducing reaction time and human error.

The figure highlights that integration is key: AI improves detection capability, while blockchain ensures trust and auditability. Together, they deliver superior performance in smart digital environments, where both rapid detection and verifiable security are essential.

5.0 Discussion

The findings collectively demonstrate that the integration of blockchain technology with intelligent security mechanisms significantly enhances system resilience, data integrity, and threat detection capabilities. When compared with existing literature, these results both confirm and extend prior research in this domain.

The substantial reduction in successful cyber-attacks as blockchain adoption increases. The decline from approximately 75% attack success in non-blockchain systems to around 12% in fully integrated environments underscores the effectiveness of decentralized security architectures. This observation is consistent with previous studies that emphasize blockchain's ability to eliminate single points of failure and enhance system trust through distributed consensus (Conti et al., 2018). Unlike traditional centralized security models, which are vulnerable to targeted attacks, blockchain-based systems distribute data across multiple nodes, making unauthorized manipulation significantly more difficult. Furthermore, the results extend earlier research by quantifying the progressive security improvement across different adoption levels, demonstrating that even partial implementation provides measurable benefits (Kassim, 2025; Islam et al., 2025).

A comparative analysis provide of data integrity across different consensus mechanisms, revealing

that blockchain-based approaches, particularly PBFT and PoS, offer superior integrity compared to centralized systems. These findings align with prior research indicating that consensus mechanisms play a critical role in ensuring data reliability and preventing tampering (Kshetri, 2018). The higher integrity scores associated with PBFT-based systems support the argument that permissioned blockchain models are particularly suitable for enterprise and smart digital environments. However, the figure also reflects a trade-off observed in previous studies: while stronger consensus mechanisms improve integrity, they may introduce scalability and performance challenges.

The study also demonstrates that hybrid cybersecurity frameworks combining blockchain and artificial intelligence achieve the highest detection accuracy and also in medicine development in healthcare system (Sami et al., 2026; Islam et al., 2026). This result is consistent with recent research highlighting the complementary strengths of AI and blockchain technologies. AI enhances anomaly detection and adaptive learning, while blockchain ensures data integrity and trustworthiness (Das et al., 2025). The superior performance of hybrid models suggests that integrated approaches are more effective than standalone systems. This finding reinforces the growing consensus that future cybersecurity solutions must combine multiple technologies to address complex and evolving threats.

Despite these advantages, the results also reflect limitations identified in previous studies. For instance, the increased computational requirements of blockchain and AI-based systems can affect performance, particularly in large-scale environments. Additionally, while blockchain improves data integrity, it does not inherently provide real-time threat detection, necessitating integration with AI-based systems (Shone et al., 2018; Ibukun & Nimotalai, 2024). These observations highlight the importance of designing optimized and scalable frameworks.

Overall, the findings confirm that blockchain-based cybersecurity frameworks offer significant improvements over traditional approaches, particularly when integrated with intelligent detection systems. The results contribute to the existing body of knowledge by providing quantitative evidence of performance improvements and emphasizing the importance of hybrid, multi-layered security architectures in modern digital environments.

6.0 Limitations

One of the most prominent limitations is scalability, particularly in large-scale digital ecosystems such as smart cities, healthcare systems, and industrial networks. Blockchain networks inherently require consensus mechanisms to validate transactions, which can introduce latency and reduce system throughput. As the number of connected devices increases, the computational and communication overhead also rises, limiting the efficiency of real-time applications. Similar scalability challenges have been observed in large-scale data-driven systems, where inefficient processing frameworks lead to performance bottlenecks (Hasan et al., 2026).

Another major limitation is the high computational and energy cost associated with blockchain operations. Consensus mechanisms such as Proof of Work (PoW) require significant processing power, making them unsuitable for resource-constrained environments. Even alternative mechanisms such as Proof of Stake (PoS) and PBFT introduce overhead that can affect system performance. This challenge parallels findings in data-intensive computational models, where increasing analytical complexity leads to higher resource consumption (Alam et al., 2025).

The integration of blockchain with artificial intelligence (AI) and big data analytics introduces additional complexities. While AI-driven models enhance threat detection and predictive capabilities, they require large volumes of high-quality data and computational resources. Moreover, these systems are vulnerable to adversarial attacks, where malicious inputs can compromise model accuracy. Studies have demonstrated that AI-based frameworks must be carefully designed to ensure robustness and interpretability in complex environments (Sikder et al., 2023a). Furthermore, the integration of multi-omics and multimodal data analytics, as explored in advanced AI frameworks, highlights the increasing

complexity of managing heterogeneous data sources securely (Sikder et al., 2023b; Mondal et al., 2026a).

Data privacy and governance also remain significant concerns in blockchain-based systems. While blockchain ensures data immutability and transparency, it may conflict with privacy requirements, particularly in sensitive domains such as healthcare and finance. The need for secure data sharing without compromising confidentiality requires advanced cryptographic techniques and governance frameworks. Research in data governance and analytics infrastructure emphasizes the importance of structured frameworks to manage data securely and efficiently (Sami et al., 2024).

Another limitation is the lack of interoperability and standardization across different blockchain platforms and digital systems. Smart environments often consist of heterogeneous technologies, including IoT devices, cloud platforms, and AI systems. Integrating these components into a unified security framework is challenging due to differences in protocols, architectures, and data formats. Similar issues have been observed in cross-domain data integration systems, where inconsistent standards hinder scalability and system interoperability (Alam et al., 2023).

Additionally, real-world implementation challenges limit the practical applicability of blockchain-based cybersecurity frameworks. Many proposed solutions are tested in controlled or simulated environments, which do not fully capture the complexities of real-world deployments. Factors such as network variability, hardware limitations, and unpredictable user behavior can significantly impact system performance. Studies integrating wearable and environmental data analytics highlight the importance of real-world validation to ensure system reliability (Nusrat et al., 2024).

7.0 Future Directions

To address these limitations, future research should focus on developing scalable, adaptive, and energy-efficient blockchain-based cybersecurity frameworks tailored for smart digital environments. The integration of AI-driven analytics with blockchain systems represents another key research area. Advanced AI frameworks, particularly those leveraging multi-omics and big data analytics, can enhance threat detection and predictive security capabilities (Mondal et al., 2026b; Hasan et al., 2026; Islam & Sinniah, 2025).

Federated learning and distributed intelligence offer promising solutions for addressing data privacy concerns. By enabling collaborative model training without sharing raw data, federated learning can enhance both security and privacy in decentralized systems. This approach aligns with emerging trends in data-driven healthcare and intelligent systems, where privacy-preserving analytics are essential (Vanu et al., 2021). Another important direction is the development of integrated hybrid security frameworks that combine blockchain, AI, and edge computing. Edge-based processing can reduce latency and improve real-time threat detection, while blockchain ensures data integrity and transparency. Such integrated systems can provide comprehensive security across multiple layers of smart digital environments (Uddin et al., 2025). Finally, future studies should emphasize real-world deployment and validation of blockchain-based cybersecurity frameworks. Large-scale experiments and field studies are necessary to evaluate system performance under realistic conditions and identify potential limitations. DataOps-oriented governance frameworks can support automated and scalable decision-making processes, enhancing system efficiency and reliability (Orthi et al., 2025).

Future directions for blockchain-based cybersecurity frameworks in securing smart digital environments will emphasize the integration of advanced technologies to achieve intelligent, scalable, and resilient security solutions. A key focus will be on combining blockchain with AI-driven models, including deep learning, transformer architectures, and continual learning systems, to enable adaptive and real-time threat detection across dynamic infrastructures (Nabi et al., 2026; Das et al., 2025; Kaur et al., 2025). The convergence of blockchain with big data analytics will further enhance predictive capabilities and support data-driven security decision-making (Ahmed et al., 2025; Rozario et al., 2025).

Additionally, future frameworks are expected to leverage edge intelligence, semantic communication, and zero-touch 6G architectures to ensure low-latency, decentralized, and automated security in next-generation networks (Varanasi et al., 2026; Mahin et al., 2026; Gangula et al., 2026).

Moreover, the development of privacy-aware governance models and lightweight blockchain mechanisms will address challenges related to data confidentiality, scalability, and resource constraints in IoT and distributed systems (Bauskar et al., 2025; Hassan et al., 2025). Cross-domain standardization and interoperability will also become essential to enable secure communication across heterogeneous smart environments. Insights drawn from machine learning applications in diverse domains such as healthcare diagnostics, imaging systems, and socio-economic analytics will continue to guide the design of robust and efficient cybersecurity frameworks capable of handling complex and large-scale data ecosystems (Manik et al., 2025; Khair et al., 2025; Bhuiyan et al., 2025). Overall, these advancements will contribute to the evolution of autonomous, intelligent, and trustworthy blockchain-based cybersecurity solutions for future smart digital environments.

8.0 Conclusion

This study demonstrates the effectiveness of blockchain-based cybersecurity frameworks in enhancing the security and resilience of smart digital environments. The analysis, supported by the three figures, highlights the critical role of decentralization, consensus mechanisms, and hybrid security models in addressing modern cybersecurity challenges. Our data shows that increasing blockchain adoption leads to a substantial reduction in successful cyberattacks, emphasizing the importance of decentralized architectures in eliminating single points of failure and improving system trust. The study reveals that advanced consensus mechanisms significantly enhance data integrity, ensuring that information remains secure and tamper-resistant across distributed networks. These findings confirm that blockchain technology provides a strong foundation for secure data management in complex digital systems. The results highlight the superiority of hybrid cybersecurity frameworks that integrate blockchain with AI-based intrusion detection systems. By combining intelligent threat detection with decentralized data validation, these models achieve the highest detection accuracy, demonstrating their effectiveness in identifying and mitigating both known and unknown cyber threats. This integration represents a significant advancement over traditional security approaches, which often rely on isolated mechanisms. In conclusion, blockchain-based cybersecurity frameworks offer a transformative approach to securing smart digital environments. By integrating decentralized technologies with intelligent analytics, these frameworks provide a robust, scalable, and adaptive solution for modern cybersecurity challenges, paving the way for more secure and resilient digital ecosystems.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

References

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

Alam, K. R., Saurav, K. R. H., Kabir, J. U. Z., Rahman, M. S., Hasan, M. I., & Barua, C. (2024). 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, 6(12), 83–102. Retrieved from https://theamericanjournals.com/index.php/tajmei/article/view/7400

Alam, M. I., Hemal, M. A. K. P., Sami, M. A., & Rahman, M. L. (2024a). Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset. European Journal of Ecology, Biology and Agriculture, 1(5), 168-184. https://doi.org/10.59324/ejeba.2024.1(5).14

Alam, M. I., Sami, M. A., Al Masud, A., Ahmed, H., & Hossain, F. (2025). AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence. Journal of Computer Science and Technology Studies, 7(11), 428-441. https://doi.org/10.32996/jcsts.2025.7.11.40

Alam, M. I., Sami, M. A., Hemal, M. A. K. P., & Rahman, M. L. (2023). Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems. Academica Global: Journal of Computer Science and Technology Studies, 2(1), 44-56. https://doi.org/10.32996/agjcsts.2023.2.1.4

Alam, M. I., Sikder, T. R., Sami, M. A., Rahman, M. L., Hemal, M. A. K. P., Linkon, A. A., Bhuiyan, M. M. R., Aziz, M. M., Islam, M. S., & Rahman, M. M. (2026). A robust and explainable approach to crop recommendation using a balanced multi-crop agronomic dataset. Journal of Environmental and Agricultural Studies, 7(3), 1-15. https://doi.org/10.32996/jeas.2026.7.3.1

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

Bhuiyan, M. M. R., Chy, M. A. R., Hossin, M. E., Rozario, E., Sultana, S., & Khair, F. B. (2025). Economic implications of homelessness in the U.S.: Applying advanced business analytics to forecast costs and develop sustainable solutions. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–5. https://doi.org/10.1109/ICECET63943.2025.11472202

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452.

Das, K., Rahman, M., & Islam, S. (2025). Hybrid blockchain-AI cybersecurity frameworks for intelligent threat detection. Journal of Cybersecurity and AI Systems, 12(3), 145–162.

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

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

Hasan, M. I., Barua, C., Rahman, M. S., Alam, K. R., Kabir, J. U. Z., & Saurav, K. R. H. (2023). Resilient Healthcare and Critical Urban Infrastructure Design Using AI-Driven Engineering and Project Management Systems . Journal of Medical and Health Studies, 4(6), 161-172. https://doi.org/10.32996/jmhs.2023.4.6.20

Hasan, M. M., Alam, M. I., Chowdhury, M. A. H., & Anwar, M. M. (2026). 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, 5(2), 41-62. https://doi.org/10.32996/jcsts.2026.5.1.5

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

Hemal, M. A. K. P., Sayeed, N., Sami, M. A., Alam, M. I., Sikder, T. R., Dipa, S. A., & Rahman, M. L. (2025). Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability. European Journal of Medical and Health Research, 3(4), 253- 263. https://doi.org/10.59324/ejmhr.2025.3(4).37

Islam, A., Rana, M. S., Karim, F., Biplob, M. Y., Sami, M. A., Rahman, M. L., & Shamarukh, S. (2026). 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, 12(5s). https://doi.org/10.29284/z691dz32

Islam, A., & Jantan, A. H. B. (2023). The mediation effect of affective organizational commitment on the relationship between HRM practices and turnover intention in the RMG industry. *Research Journal in Business and Economics*, *1*(1), 24-38.

Islam, A., Jantan, A. H. B., Khalifa, G. S., Islam, A., Islam, B., & Hossian, A. (2023). Effects of Decision Making and Work-life Balance on Productivity of Female Employees in the RMG Industry of Bangladesh. The Mediating Role of Work Motivation. *Research Journal in Business and Economics*, *1*(1), 48-59.

Islam, M. A., Islam, M. A., Amin, M. B., Hossain, M. M., Hassan, M. S., Afrin, S., & Oláh, J. (2025). Enhancing academic's performance: Exploring the interaction of innovative work behavior, intrinsic motivation, and self-efficacy in public universities. *Social Sciences & Humanities Open*, *12*, 102210.

Islam, M. A., & Sinniah, S. (2025). Exploring customer relationship management factors, customer trust, and innovation capacity: A quantitative study on customer retention. *Accountancy Business and the Public Interest*, *41*(10), 12-29.

Ibukun, K., & Nimotalai, K. O. (2024). A Comparative Analysis of the Cost-Effectiveness of Universal Health Coverage (UHC) Financing Models and Their Policy Implications in Low-and Middle-Income Countries. *Journal of Medical Science, Biology, and Chemistry*, *1*(1), 37-45.

Kabir, J. U. Z., Saurav, K. R. H., Rahman, M. S., Hasan, M. I., Barua, C., Alam, K. R., & Rahman, M. M. (2023). 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, 1(3), 144-150. https://doi.org/10.59324/ejmhr.2023.1(3).24

Kassim, N. O. (2025). Community-Driven Behavioral Intelligence Framework Strengthening US Public Health Systems, Violence Prevention, and Nationwide Community Resilience Initiatives.

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

Khair, F. B., Saimon, A. S. M., Hossain, S., et al. (2025). Deep neural network-based imaging system for efficient pancreatic tumor identification. Intelligent Decision Technologies, 19(6), 4118–4129. https://doi.org/10.1177/18724981251381581

Kassim, N. O. (2026). Assessing Mental Health Awareness and Stigma in Hartford, Connecticut, USA. *Annals of Innovation in Medicine*, *4*(1).

Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity. Computer, 51(9), 68–72.

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

Manik, M. M. T. G., Saimon, A. S. M., Ahmed, M. K., Hossain, S., Moniruzzaman, M., & Islam, M. S. (2025). Predictive modelling for early detection of type 2 diabetes using AI-driven machine learning algorithms and big data analytics. In J. C. Bansal, P. Jamwal, & S. Hussain (Eds.), Lecture Notes in Networks and Systems (Vol. 1629). Springer. https://doi.org/10.1007/978-3-032-05548-4_33

Mondal, R. S., Ahmed, R. A., Hemal, M. A. K. P., Sikder, T. R., & Juie, B. J. A. (2026a). 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, 8(2), 113–127. https://doi.org/10.37547/tajmspr/Volume08Issssue02-17

Mondal, R. S., Purba, T. N., Purba, N. N., Rahman, M. M., & Sikder, T. R. (2026b). AI-Driven Glycemic Instability Risk Modeling for Proactive Intervention and Chronic Disease Management in U.S. Healthcare Systems . Journal of Medical and Health Studies, 7(1), 29-43. https://doi.org/10.32996/jmhs.2023.4.6.21

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

Nusrat, S., Hossain, F., & Sikder, T. R. (2024). Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention. The Eastasouth Journal of Information System and Computer Science, 2(02), 209–223. https://doi.org/10.58812/esiscs.v2i02.868

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

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

Sami, M. A., Hemal, M. A. K. P., Alam, M. I., & Rahman, M. L. (2024). Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs. European Journal of Applied Science, Engineering and Technology, 2(2), 388-403. https://doi.org/10.59324/ejaset.2024.2(2).28

Sami, M. A., Rahman, M. L., Tanni, Z. A., Munmun, Z. S., Nusrat, S., & Biswas, B. (2026). Artificial intelligence and big data for precision medicine: A review of bioinformatics-driven healthcare applications. Frontiers in Computer Science and Artificial Intelligence, 5(6), 36–43. https://doi.org/10.32996/fcsai.2026.5.6.7

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach for intrusion detection system. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

Sikder, T. R., Dash, S., Uddin, B., & Hossain, F. (2023a). 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, 1(02), 153–170. https://doi.org/10.58812/esiscs.v1i02.838

Sikder, T. R., Sayeed, N., Hossain, M. J., Faruk, M. I., Alam, M. I., Uddin, S. M. M., & Adnan, M. (2025). 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, 11(4). https://doi.org/10.22399/ijcesen.4533

Sikder, T. R., Siam, M. A., Melon, M. M. H., Uddin, S. M. M., Mohonta, S. C., & Karim, F. (2023b). A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion. Journal of Computer Science and Technology Studies, 5(3), 183-188. https://doi.org/10.32996/jcsts.2023.5.3.13

Uddin, S. M. M., Chy, M. A. R., Sikder, T. R., Faruk, M. I., Adnan, M., & Hossain, M. J. (2025). Bio-Cognitive AI Systems for Predictive Healthcare Decision Support. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-9. https://doi.org/10.1109/ICAFT66710.2025.11453175.

Vanu, N., Hasan, M. R., Sikder, T. R., & Tamanna, Z. S. (2021). 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, 3(2), 124-141. https://doi.org/10.32996/jcsts.2021.3.2.11

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