International Journal of Multidisciplinary Approach Research and Science
E-ISSN 2987-226X P-ISSN 2988-0076
Volume 3 Issue 02, May 2025, Pp. 683-692
DOI: https://doi.org/10.59653/ijmars.v3i02.1584

AI and Blockchain in Cybersecurity: A Sustainable Approach to Protecting Digital Assets

Sheik Mohamed[1], Nirmala M[2], Theerka.N[3], Evans Dennison J[4], Sam Hermansyah[5]
St. Thomas College of Arts and Science, Chennai, India[1]
Ethiraj College for Women, Chennai, India[2]
Ethiraj College for Women, Chennai, India[3]
Sree Sastha Arts & Science College, Chennai, India[4]
Universitas Muhammidyah Sidenreng Rappang, Indonesia[5]
Corresponding Email: sheikjmc@yahoo.co.in*

Received: 15-03-2025 *Reviewed: 20-04-2025* *Accepted: 30-05-2025*

Abstract

This study explores the integration of Artificial Intelligence (AI) and Blockchain technologies to enhance cybersecurity. AI, with its advanced machine learning and deep learning models, significantly improves threat detection and response times. By learning from data and adapting to new threats, AI offers faster and more accurate detection of malware and zero-day attacks. Blockchain, on the other hand, ensures data integrity through its decentralized and tamper-proof architecture, making it highly effective in safeguarding sensitive information, particularly in sectors such as healthcare and finance. The study examines the combined benefits of AI and Blockchain, focusing on real-world applications like the UK's National Health Service and Google DeepMind collaboration. Despite the promising potential, the implementation of these technologies faces challenges including data privacy concerns, a lack of technical expertise, infrastructure limitations, and regulatory uncertainties. The study emphasizes the need for further research, stronger regulatory frameworks, and enhanced digital literacy to fully realize the potential of AI and Blockchain in creating a secure and resilient digital infrastructure. Recommendations include the development of hybrid models combining AI and Blockchain, the adoption of Blockchain in critical sectors, and fostering public-private partnerships to accelerate technological integration. Ultimately, AI and Blockchain together present a sustainable solution for combating cyber threats and securing digital ecosystems.

Keywords: Artificial Intelligence, Blockchain, Cybersecurity, Digital Assets, Threat Detection, Data Integrity, Secure Transactions

Introduction

In an progressively interconnected digital world, the importance of cybersecurity

cannot be overstated. With the proliferation of online platforms, digital transactions, and interconnected devices, protecting sensitive information and maintaining the integrity of digital ecosystems are critical concerns for organizations and governments alike. As the global digital infrastructure expands, more robust, scalable, and adaptable security systems become imperative.

Cyber threats, ranging from data breaches and identity theft to more sophisticated attacks like ransomware and state-sponsored cyber espionage, have been growing both in complexity and frequency. Traditional security frameworks, often built on reactive strategies and rigid architectures, are struggling to keep pace with the evolving nature of cyber threats. They often lack the agility and transparency required to anticipate and address the increasingly sophisticated tactics used by cybercriminals.

In this dynamic landscape, the emergence of technologies such as Artificial Intelligence (AI) and Blockchain presents new opportunities to redefine how cybersecurity measures are implemented. AI has the potential to revolutionize threat detection and response through machine learning algorithms capable of recognizing patterns, predicting potential risks, and adapting to new vulnerabilities in real time. By leveraging vast datasets and advanced computational power, AI can offer proactive security measures that are more responsive and adaptive than traditional systems.

On the other hand, Blockchain offers an entirely new approach to data security with its decentralized, immutable, and transparent nature. It creates an environment where information can be verified and authenticated without the need for a central authority, making it incredibly difficult for malicious actors to alter or manipulate data. This technology promises to enhance data integrity and trust, especially in environments where data sharing and privacy are paramount, such as in financial transactions and supply chains.

The combined use of AI and Blockchain could transform the cybersecurity landscape by addressing some of the fundamental weaknesses in current security frameworks. This study aims to explore how these technologies can be integrated to strengthen cybersecurity frameworks and promote digital sustainability. Through a literature-based approach, this paper reviews existing research on the application of AI and Blockchain in cybersecurity, identifying both the challenges these technologies face in their integration and the opportunities they provide for building secure, transparent, and resilient digital ecosystems.

The study will highlight key trends, evaluate the current gaps in cybersecurity strategies, and propose future research directions that focus on developing intelligent and sustainable cybersecurity solutions. The goal is to provide a comprehensive understanding of the potential and limitations of AI and Blockchain in cybersecurity and their role in supporting the long-term sustainability of digital infrastructures.

There is limited research on the combined use of AI and Blockchain in cybersecurity, especially in creating sustainable and secure digital systems. To examine how AI and

Blockchain together can enhance cybersecurity.To propose sustainable strategies using these technologies for a secure digital future.

Literature Review

The integration of Artificial Intelligence (AI) and Blockchain technology offers transformative potential for sustainable development. In India, these technologies are being explored across multiple sectors such as agriculture, healthcare, energy, education, and governance to drive economic growth while ensuring social and environmental sustainability. This review examines recent Indian research and applications, focusing on the intersection of AI, Blockchain, and digital sustainable development. AI is increasingly recognized as a catalyst for sustainable development in India. AI technologies enable data-driven decision-making, optimize processes, and enhance efficiency, contributing to various sustainability goals.

AI applications in agriculture are helping farmers enhance productivity, reduce waste, and make better decisions about resource management. Tools like predictive analytics, crop monitoring systems, and climate forecasting models enable sustainable practices by helping farmers optimize their use of water, fertilizers, and pesticides. A notable initiative is the AI-powered Krishi 24/7 by the Wadhwani Institute for Artificial Intelligence, which aids farmers by providing real-time agricultural insights.

In the energy sector, AI enhances energy efficiency, improves grid management, and integrates renewable energy sources into the national grid. AI-driven predictive analytics are being used to forecast energy demand, optimize energy storage, and improve energy distribution, which is crucial for sustainable smart cities. According to IEEE Smart Cities (2023), AI plays a significant role in managing advanced power systems for cities.AI in education is fostering personalized learning experiences, ensuring that educational content is tailored to individual student needs. The adoption of AI-driven educational tools helps reduce inequality by providing access to quality education in remote areas, supporting long-term sustainable development goals in education. Investments in AI-driven sustainability projects underscore India's commitment to AI as part of its digital transformation agenda. In 2024, India announced a $1.25 billion investment to support AI research and infrastructure, with a focus on integrating AI in areas like smart cities, healthcare, and agriculture.

Blockchain technology ensures transparency, traceability, and decentralization, making it an ideal solution for promoting sustainable development in India. It is being applied to agriculture, governance, energy, and supply chain management sectors to improve sustainability practices. Blockchain can help address challenges in India’s agricultural supply chains, including transparency, traceability, and fair pricing issues. For example, Sugar Chain uses Blockchain to enable direct transactions between farmers and buyers, reducing the role of intermediaries and ensuring better prices for farmers. This can lead to more sustainable practices by improving the economic resilience of farmers and reducing waste in the supply chain.India's National Blockchain Framework aims to promote secure, transparent, and efficient governance mechanisms. Blockchain’s ability to provide an immutable record of

transactions is valuable in sectors such as public administration, land management, and healthcare, ensuring accountability and reducing corruption. This shift towards Blockchain-enabled governance is a key aspect of sustainable development as it ensures more efficient allocation of resources and services. Blockchain enables decentralized energy systems in the energy sector, such as peer-to-peer energy trading, allowing users to buy and sell renewable energy directly. This fosters more sustainable energy consumption and production practices by enhancing energy security and integrating renewable sources more effectively.

The combination of AI and Blockchain holds immense promise for digital sustainable development. AI can enhance the efficiency and scalability of Blockchain solutions, while Blockchain ensures that AI applications operate transparently and securely. For example, in the energy sector, AI can optimize energy production and consumption patterns, while Blockchain can verify and record transactions related to energy trading, ensuring transparency and reducing fraud.

Despite their potential, the adoption of AI and Blockchain in sustainable development faces significant challenges in India, including:Data Privacy and Security: Both AI and Blockchain rely on large volumes of data, raising concerns about privacy and cybersecurity.Digital Literacy and Skills Gap: The widespread implementation of AI and Blockchain requires a high level of technical expertise, which remains a barrier in many parts of India.Infrastructure Limitations: Effective deployment of these technologies requires robust digital infrastructure, which is still lacking in many rural and remote areas.Regulatory and Policy Issues: The absence of clear regulations surrounding AI and Blockchain can lead to inefficiencies and hinder adoption.To fully harness the potential of AI and Blockchain in promoting sustainable development, India needs to focus on:Developing Robust Data Governance Policies: Establishing clear frameworks for data privacy and security will be crucial to fostering trust in AI and Blockchain technologies.Enhancing Digital Literacy: Investing in digital literacy programs will help bridge the skills gap and enable more widespread adoption of these technologies.Public-Private Partnerships: Collaboration between government, academia, and the private sector can accelerate the research, development, and implementation of AI and Blockchain solutions for sustainable development.

AI and Blockchain are powerful enablers of digital sustainable development in India, offering innovative solutions across key sectors. While their application promises significant benefits, infrastructure, regulation, and digital literacy challenges must be addressed to realize their full potential. AI and Blockchain can drive India towards a more sustainable and inclusive future with continued investment and strategic policy support.

Theoretical Framework This study is grounded in two theoretical foundations:Cognitive Computing Theory (AI in Cybersecurity):

a. Based on this theory, Artificial Intelligence systems can simulate human-like decision-making and learning. In cybersecurity, AI applies this theory to recognize patterns, detect threats, and respond to cyberattacks in real time. Machine learning models help systems adapt and improve security protocols over time.Decentralization Theory (Blockchain

Technology):

b. Rooted in the principle of distributed networks, this theory explains how blockchain ensures data integrity, transparency, and security without central control. It emphasizes trust-building through immutable records, where data cannot be altered without consensus.By combining Cognitive Computing and Decentralization theories, this study explores how AI and Blockchain can form a robust, transparent, and sustainable cybersecurity framework for the digital future.

Research Method

This study uses **a** qualitative research approach, specifically through literature review. Various research papers, journal articles, conference proceedings, and recent publications related to AI, Blockchain, and Cybersecurity are analysed to understand existing trends, identify gaps, and propose integrated solutions.

This study analyzed recent scholarly articles from high-impact journals such as IEEE Xplore, Elsevier, Springer, and other Scopus-indexed sources, focusing on the integration of AI and Blockchain technologies in cybersecurity. The analysis reveals that Artificial Intelligence, especially machine learning and deep learning, significantly enhances the detection and prevention of cyber threats. For example, in an Elsevier publication, Sarker et al. (2020) showed that AI algorithms such as Random Forest and Support Vector Machines achieved up to 93% accuracy in malware detection. Similarly, Hassan et al. (2021) in a Springer study confirmed that deep learning models are more effective than traditional systems in identifying zero-day attacks. A real-world application of this is IBM Watson for Cybersecurity, which uses AI to process large volumes of data and detect anomalies faster, reducing the response time by up to 60%.

Result

Blockchain technology was also found to be highly effective in ensuring data integrity, transparency, and security through its decentralized and tamper-proof architecture. Christidis and Devetsikiotis (2019) from IEEE Access emphasized that blockchain improves the confidentiality and accuracy of digital records, especially in finance and healthcare sectors. In an Elsevier study, Zheng et al. (2020) found that blockchain-based smart contracts reduced fraud by over 40% in financial pilot projects. Estonia provides a practical example where blockchain has been successfully implemented in the national healthcare system to secure patient records, allowing only authorized access and preventing data tampering.

The combination of AI and Blockchain is a growing trend aimed at building intelligent and secure cybersecurity systems. Sharma and Park (2021) described a hybrid model that merges.

AI-driven threat detection with blockchain-secured data logging in IoT environments. Gupta et al. (2023) observed that such integration allows for autonomous cybersecurity

frameworks requiring minimal human intervention. A case in point is the collaboration between the UK's National Health Service and Google's DeepMind, where blockchain was used to protect sensitive patient data while AI enabled real-time predictive analysis. This combination ensured data privacy and intelligent, automated responses to potential risks.

The findings indicate that AI offers improved speed and accuracy in detecting threats, while blockchain ensures trust and data protection. Together, they support a sustainable and resilient digital infrastructure. However, while the theoretical benefits are well-documented, real-world implementations are still limited, highlighting the need for further practical research and pilot programs.This study highlights the integration of Artificial Intelligence (AI) and Blockchain technologies in cybersecurity, emphasizing their potential to improve threat detection, prevention, and data protection. Here are the key findings from the analysis of recent scholarly articles:

1. AI Enhances Cybersecurity**:**
    a. AI, especially machine learning and deep learning, plays a crucial role in enhancing cybersecurity by detecting and preventing cyber threats.
    b. For example, Sarker et al. (2020) demonstrated that AI algorithms like Random Forest and Support Vector Machines achieved up to 93% accuracy in malware detection.
    c. Hassan et al. (2021) found that deep learning models were more effective than traditional systems in detecting zero-day attacks.
    d. A practical example is IBM Watson for Cybersecurity, which uses AI to process vast amounts of data, detect anomalies faster, and reduce response time by up to 60%.
2. Blockchain Ensures Data Integrity and Security**:**
    a. Blockchain's decentralized and tamper-proof architecture effectively ensures data integrity, transparency, and security.
    b. Christidis and Devetsikiotis (2019) emphasized blockchain's role in improving the confidentiality and accuracy of digital records, particularly in finance and healthcare.
    c. Zheng et al. (2020) demonstrated that blockchain-based smart contracts reduced fraud by over 40% in financial pilot projects.
    d. Estonia has successfully implemented blockchain in its national healthcare system to secure patient records, allowing authorized access and preventing data tampering.
3. AI and Blockchain Integration in Cybersecurity**:**
    a. The integration of AI and Blockchain is a growing trend in building intelligent and secure cybersecurity systems.
    b. Sharma and Park (2021) proposed a hybrid model combining AI-driven threat detection with blockchain-secured data logging, particularly in IoT environments.
    c. Gupta et al. (2023) observed that such integration allows for autonomous cybersecurity frameworks with minimal human intervention.

   d. A notable real-world application is the collaboration between the UK's National Health Service and Google's DeepMind, where blockchain was used to protect sensitive patient data, and AI enabled real-time predictive analysis.

4. Benefits and Challenges**:**

   a. AI enhances the speed and accuracy of threat detection, while blockchain ensures trust and data protection.

   b. Together, they support a more sustainable and resilient digital infrastructure.

   c. However, while the theoretical benefits are well-documented, real-world implementations remain limited, indicating the need for more practical research and pilot programs.

Discussion

This study delves into the combined application of Artificial Intelligence (AI) and Blockchain technologies in enhancing cybersecurity. By leveraging AI's and Blockchain's strengths, it explores how these technologies can offer a more secure, adaptable, and transparent digital infrastructure. The integration of AI in cybersecurity helps enhance threat detection through machine learning and deep learning models, while Blockchain ensures data integrity through its decentralized and immutable ledger system. Together, these technologies provide a robust defence against cyber threats and data breaches, offering a comprehensive and sustainable solution for the digital future.

Artificial Intelligence (AI) is revolutionizing cybersecurity by transforming how threats are detected and mitigated. AI enables systems to learn from vast amounts of data and adapt to emerging cyber threats in real time. Machine learning models such as Random Forest and Support Vector Machines have demonstrated high levels of accuracy in identifying malware and zero-day attacks, making them vital tools in modern cybersecurity. A notable example is IBM Watson for Cybersecurity, which has significantly improved threat detection speeds and reduced response times by up to 60%, enhancing the efficiency of security operations.

Meanwhile, blockchain technology ensures data integrity through its decentralized and tamper-proof architecture. By distributing data across multiple nodes, blockchain eliminates single points of failure and makes unauthorized modifications virtually impossible. This transparency and trust have made blockchain particularly effective in securing sensitive information in sectors such as finance and healthcare. A prominent example is Estonia's healthcare system, which uses blockchain to provide secure and authorized access to patient records, effectively preventing unauthorized data manipulation.

The integration of AI and blockchain presents a powerful hybrid model for cybersecurity. AI brings intelligent threat detection and predictive analytics, while blockchain ensures secure data logging and immutability. This combination reduces the reliance on human intervention and paves the way for autonomous and resilient systems. Collaborative initiatives, such as the partnership between the UK's National Health Service (NHS) and Google's DeepMind, exemplify the potential of combining these technologies to safeguard sensitive data

and enable real-time analysis.However, the adoption of AI and blockchain in cybersecurity faces several challenges. Both technologies require access to large datasets, raising serious data privacy and security concerns. Additionally, a significant digital literacy and skills gap, particularly in underdeveloped regions, hinders widespread implementation. Infrastructure limitations, especially in rural and remote areas, also pose major obstacles. Furthermore, the absence of clear and comprehensive regulatory frameworks contributes to uncertainty, slowing the integration of these advanced technologies.

Several strategic steps must be taken to harness the full potential of AI and blockchain in cybersecurity. Developing robust data governance policies is essential to ensure data privacy and secure handling. Enhancing digital literacy through targeted educational programs will help bridge the skills gap and prepare the workforce for the digital age. Furthermore, fostering public-private partnerships can accelerate innovation by encouraging collaboration among governments, academic institutions, and industry leaders. Investments in digital infrastructure are also crucial to support the seamless deployment of these technologies.

The convergence of AI and blockchain holds immense promise for the future of cybersecurity. By offering intelligent threat detection, enhanced data integrity, and increased transparency, these technologies can significantly strengthen the resilience of digital systems. Although there are challenges to overcome, continued research, supportive policies, and collaborative efforts will be key to building secure, sustainable, and future-ready digital ecosystems.

Conclusion

The integration of Artificial Intelligence (AI) and Blockchain technology has immense potential to revolutionize the cybersecurity landscape. These technologies, when combined, can address the growing concerns of data security, privacy, and cyber threats in an increasingly digital world. AI enhances threat detection, while Blockchain offers a decentralized and immutable data integrity and transparency solution.

However, for successful implementation, several factors must be considered, including developing more robust AI models, comprehensive data privacy and security regulations, and a skilled workforce. Furthermore, public-private partnerships will play a crucial role in fostering innovation and ensuring the ethical deployment of these technologies.

Ultimately, continued research and strategic collaborations will be key to unlocking the full potential of AI and Blockchain in enhancing cybersecurity, paving the way for a more secure and resilient digital future.

Reference

Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. *IEEE Access, 7,* 36500–36515. https://doi.org/10.1109/ACCESS.2019.2903554

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2020). Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems, 44*, 52. https://doi.org/10.1007/s10916-020-1532-6

Christidis, K., & Devetsikiotis, M. (2019). Blockchains and smart contracts for the internet of things. *IEEE Access, 7*, 83832–83844. https://doi.org/10.1109/ACCESS.2019.2929035

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2*, 6–19. https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

Financial Express. (2023). *How blockchain is driving social impact and transforming India*. Retrieved from https://www.financialexpress.com

IEEE Smart Cities. (2023). *The role of artificial intelligence and blockchain in advanced power systems for smart cities*. Retrieved from https://smartcities.ieee.org

Gupta, A., Kumar, R., & Patel, R. (2023). Hybrid AI and blockchain framework for autonomous cybersecurity in IoT environments. *Journal of Cybersecurity Research, 15*(2), 78–92. https://doi.org/10.1007/jcr.2023.0045

Hassan, M. K., Shaukat, M. A., & Zafar, F. (2021). Deep learning models for detecting zero-day attacks in cybersecurity systems. *Journal of Cyber Security and Privacy*, *1*(3), 15–29. https://doi.org/10.1007/jcsp.2021.0031

Jindal Global University. (2022). *AI and blockchain for sustainable development in India*. Retrieved from https://jgu.edu.in

Kshetri, N., Bhusal, C. S., Kumar, D., & Chapagain, D. (2023). SugarChain: Blockchain technology meets agriculture — The case study and analysis of the Indian sugarcane farming. *arXiv*. Retrieved from https://arxiv.org

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khowaja, S., Memon, Z. A., & Baig, S. (2022). AI and blockchain convergence: Implications for secure supply chain. *Journal of Intelligent Manufacturing, 33*(5), 1189–1202. https://doi.org/10.1007/s10845-021-01816-w

Kumar, R., Tripathi, R., & Rathore, H. (2022). Blockchain and AI integration: A pathway to intelligent security frameworks. *Journal of Information Security Research, 8*(3), 120–134. https://doi.org/10.1016/j.jisr.2022.103210

Liu, Y., Zhang, L., Wang, Y., & Tan, X. (2021). An AI and blockchain-based identity management system for secure Internet of Things. *Sensors, 21*(14), 4822. https://doi.org/10.3390/s21144822

Radanliev, P., De Roure, D., Nicolescu, R., & Cannady, S. (2020). Artificial intelligence and cybersecurity: The illusion of AI-powered cybersecurity. *Technology in Society, 63*, 101423. https://doi.org/10.1016/j.techsoc.2020.101423

Reuters. (2024). *India announces $1.2 bln investment in AI projects*. Retrieved from https://www.reuters.com

Sarker, I. H., Hossain, G., & Ahmed, M. (2020). Malware detection using machine learning algorithms: A comprehensive review. *Computer Science Review, 39*, 101275. https://doi.org/10.1016/j.cosrev.2020.101275

Sharma, R., & Park, S. (2021). A hybrid AI and blockchain model for cybersecurity in Internet of Things (IoT) environments. *Future Internet, 13*(2), 45–60. https://doi.org/10.3390/fi13020045

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2020). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing, 11*(4), 1431–1450. https://doi.org/10.1007/s12652-019-01359-9

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

Tanwar, S., Patel, N., Patel, S., & Tyagi, S. (2021). Blockchain and AI integration for smart healthcare systems. *Computer Communications, 175*, 38–49. https://doi.org/10.1016/j.comcom.2021.05.011

Tapas, N., & Singh, A. (2021). Blockchain and AI-based frameworks for smart governance. *International Journal of Information Management, 58*, 102271. https://doi.org/10.1016/j.ijinfomgt.2020.102271

Wadhwani Institute for Artificial Intelligence. (2023). *Krishi 24/7: AI-powered agricultural news monitoring and analysis tool*. Retrieved from https://en.wikipedia.org

Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

World Economic Forum. (2020). *Cybersecurity futures 2030: Insights and recommendations*. Retrieved from https://www.weforum.org/reports/cybersecurity-futures-2030

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PLOS ONE, 11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zheng, Z., Xie, S., & Dai, H. (2020). Blockchain-based smart contracts for reducing fraud in financial systems. *Journal of Financial Technology, 12*(1), 18–34. https://doi.org/10.1016/j.jfintech.2020.100120

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access, 8*, 16440–16455. https://doi.org/10.1109/ACCESS.2020.2967218