ADI Journal on Recent Innovation (AJRI)
Vol. 7, No. 2, 2026, pp. 197−208
E-ISSN: 2686-0384 | P-ISSN: 2685-9106, DOI: 10.34306

Blockchain Augmented AI Architecture for Strengthening Cybersecurity and Operational Trust in Modern Business Ecosystems

Bunga Novriyanti[1*], Mardiana[2], Ninda Lutfiani[3], Kgomotso Moyo[4]
[1]Department of Accounting, Bank Negara Indonesia, Indonesia
[2]Faculty of Economics and Business, University of Raharja, Indonesia
[3]Doctor of Computer Science, Satya Wacana Christian University, Indonesia
[4]Mfinitee Incorporation, South Africa
[1]bunga.novriyanti@raharja.info, [2]mardiana@raharja.info, [3]982022020@student.uksw.edu, [4]kgomotsoo.m@mfinitee.co.za
***Corresponding Author**

Article Info

Article history:

Submission October 28, 2025
Revised December 25, 2025
Accepted February 27, 2026
Published March 16, 2026

Keywords:

Blockchain Integration
Artificial Intelligence
Cybersecurity
Operational Trust
Digital Business Ecosystems

ABSTRACT

Modern enterprises increasingly rely on interconnected digital infrastructures, which significantly increase exposure to cyber threats and trust-related vulnerabilities. Traditional security mechanisms often face limitations in providing real-time detection, transparent data validation, and resilient protection across distributed environments. **This study** aims to develop and evaluate a Blockchain-Augmented AI Architecture to enhance cybersecurity performance and strengthen operational trust within digital business ecosystems. **The research** adopts a quantitative experimental approach by integrating machine learning–based anomaly detection with a private blockchain layer for secure event logging and tamper-proof verification. The system is tested using simulated enterprise network traffic, and performance is evaluated based on detection accuracy, latency, throughput, and integrity validation efficiency. A comparative analysis is also conducted against conventional centralized cybersecurity models. **The results** demonstrate that the proposed architecture significantly improves cybersecurity robustness, achieving higher anomaly detection accuracy, reduced false positives, and faster verification time compared to baseline models. Additionally, blockchain integration enhances operational trust by ensuring immutable audit trails, decentralized consensus, and transparent data provenance. **Overall**, the combined system exhibits superior reliability and resilience across simulated network scenarios. This study concludes that integrating AI-driven detection with blockchain technology provides a more secure, transparent, and trustworthy cybersecurity framework for modern enterprises, while offering strong potential to support scalable digital transformation and address emerging threats in distributed environments.

DOI: https://doi.org/10.34306/ajri.v7i2.1384

1. INTRODUCTION

The rapid acceleration of digital transformation across global industries has significantly increased organizational dependence on interconnected systems, cloud infrastructures, and automated business operations.

While these technologies enhance efficiency, scalability, and operational agility, they simultaneously expand the attack surface for cyber threats [1]. Modern enterprises now face increasingly complex security challenges, including ransomware attacks, data breaches, and sophisticated supply chain intrusions. These evolving threats expose critical weaknesses in traditional centralized security architectures, which often lack adaptability, transparency, and resilience in highly distributed digital environments [2].

As business ecosystems become more data-driven and decentralized, the limitations of conventional cybersecurity approaches become increasingly evident. Centralized security mechanisms are prone to single points of failure, delayed threat detection, and limited auditability, making them insufficient for safeguarding modern digital infrastructures [3]. Consequently, organizations require advanced security solutions capable of real-time threat identification, verifiable data integrity, and resilient system protection. The growing demand for secure, transparent, and trustworthy digital infrastructures highlights the urgency of rethinking cybersecurity strategies in the context of large-scale digital transformation [4].

In response to these challenges, emerging technologies such as Artificial Intelligence (AI) and blockchain have gained significant attention for their complementary capabilities in cybersecurity enhancement [5]. AI-driven anomaly detection enables intelligent analysis of network traffic and facilitates rapid identification of malicious behavior, while blockchain technology provides immutable, decentralized mechanisms for ensuring data integrity and trust. By combining predictive intelligence with cryptographic verification, the integration of AI and blockchain presents a promising pathway to overcome the inherent weaknesses of traditional security systems [6]. This convergence aligns with global priorities for responsible and secure technological development, particularly as cyber risks increasingly threaten sustainable digital growth.

Furthermore, the adoption of secure and trustworthy digital infrastructures contributes directly to broader societal and economic objectives, including the United Nations Sustainable Development Goals (SDGs), notably SDG 9 (Industry, Innovation, and Infrastructure) and SDG 16 (Peace, Justice, and Strong Institutions). Strengthening cybersecurity and ensuring data integrity support resilient industrial systems, enhance institutional governance, and promote ethical digital transformation [7]. Within this context, this study proposes a Blockchain-Augmented AI Architecture designed to enhance cybersecurity robustness and operational trust in modern business ecosystems. By integrating AI-based anomaly detection with blockchain-enabled verification, the proposed framework offers a scalable, transparent, and resilient solution for addressing emerging cyber threats while supporting long-term digital sustainability [8].

2. RESEARCH METHOD

This study adopts a structured and systematic research methodology to evaluate the effectiveness of a Blockchain-Augmented AI Architecture in enhancing cybersecurity and operational trust within digital business ecosystems. The methodological framework is designed to ensure rigor, transparency, and replicability by integrating theoretical exploration, system development, experimental evaluation, and statistical analysis [9]. Through a quantitative experimental approach, the research compares a conventional centralized cybersecurity model with the proposed blockchain-enhanced architecture under controlled conditions. The following subsections outline the literature foundation, research design, data collection process, system development procedures, evaluation metrics, and analytical techniques employed to comprehensively assess system performance and trust validation [10].

2.1. Literature Review

The literature review examines the theoretical foundations, technological developments, and empirical findings related to AI-driven cybersecurity, blockchain-based security mechanisms, and hybrid architectures that integrate both technologies [11]. Prior studies demonstrate that machine learning models such as Random Forest, Support Vector Machine, and Long Short-Term Memory (LSTM) are effective in detecting anomalous network behavior through supervised and unsupervised learning approaches by analyzing complex traffic patterns. Despite their strong analytical capabilities, conventional AI-based cybersecurity systems remain vulnerable to data tampering, single points of failure, and limited transparency in auditability and decision-making processes, which reduces trust in centralized security environments [12]. In contrast, blockchain technology has been widely recognized for enhancing data integrity, traceability, and operational trust through decentralized and immutable verification mechanisms. However, blockchain systems also face limitations, including computational overhead, latency, scalability constraints, and the absence of inherent real-time threat detection when deployed independently.

Recent scholarly research therefore emphasizes the integration of AI and blockchain as a promising solution to address the limitations of standalone approaches [13]. By combining AI-driven anomaly detection with blockchain-enabled validation, hybrid architectures aim to provide intelligent threat identification alongside tamper-resistant and transparent security logging. Nevertheless, many existing studies remain limited to conceptual models or partial evaluations, lacking comprehensive performance benchmarking, architectural optimization, and systematic assessment within enterprise-scale environments. Addressing these gaps, this study evaluates a Blockchain-Augmented AI Architecture designed to enhance cybersecurity resilience and operational trust by benchmarking detection performance, system efficiency, and blockchain-based integrity validation within modern digital business ecosystems [14].

2.2. Research Design

This study employs a quantitative experimental research design to systematically compare the performance of a traditional centralized cybersecurity model with the proposed Blockchain-Augmented AI Architecture [15]. The research begins with the development of both systems under identical technical configurations, where the baseline model represents conventional centralized detection, while the proposed architecture integrates machine learning–based anomaly detection with a private blockchain for verification and immutable logging [16]. Controlled network simulations are then constructed to replicate realistic enterprise environments, including normal traffic, known cyberattacks, and hybrid threat scenarios. This ensures that both models are evaluated under comparable and comprehensive conditions.

Performance benchmarking is conducted by measuring detection accuracy, false positive rates, latency, throughput, and the efficiency of blockchain-based integrity validation [17]. Additional indicators related to operational trust, such as auditability and data immutability, are assessed through blockchain event logs. To ensure the reliability of results, statistical validation techniques such as paired t-tests or ANOVA are applied to determine whether observed improvements are significant. This two-stage approach allows the research to objectively determine the extent to which blockchain integration enhances AI-driven cybersecurity and strengthens trust within digital business ecosystems [18].

2.3. Data Collection

The data used in this study were obtained from simulated enterprise network traffic, publicly available cybersecurity datasets, and blockchain event logs generated during system operation. Simulated traffic was produced using tools such as CICFlowMeter to reflect realistic organizational environments, while public datasets, including CICIDS 2017 and UNSW-NB15, were utilized to provide diverse and well-labeled attack scenarios, thereby enhancing the reliability of the anomaly detection models [19]. Blockchain event logs captured smart contract executions, transactions, block creation, and validation activities, offering insights into transparency and auditability. Prior to analysis, all data underwent preprocessing steps such as noise removal, normalization, categorical encoding, missing value handling, and class balancing to ensure data quality, reduce bias, and support effective anomaly detection and reliable evaluation of the proposed Blockchain-Augmented AI Architecture [20].

Table 1. Dataset Characteristics and Preprocessing

Traffic Type	Source	Records	Preprocessing
Normal	Enterprise Simulation	50,000	Cleaning, normalization
Attack	Attack Scenarios	30,000	Labeling, scaling
Encrypted	Secure Communication	20,000	Feature extraction
Mixed	Combined Traffic	40,000	Balancing, deduplication

Table 1 summarizes the main characteristics of the datasets used in this study along with the corresponding preprocessing steps. The dataset consists of various traffic types, including normal, attack, encrypted, and mixed traffic, generated from simulated enterprise environments to reflect realistic network conditions. Appropriate preprocessing techniques such as data cleaning, normalization, feature extraction, and balancing are applied to ensure data quality and consistency prior to model training and evaluation, thereby supporting reliable and unbiased performance assessment [21].

2.4. System Development Procedure

The system development procedure outlines the step-by-step construction of the Blockchain-Augmented AI Architecture, beginning from the formation of the anomaly detection engine, followed by the establishment of the blockchain-based validation mechanism, and finalized through the integration of both components into a unified operational framework. This procedure ensures that each computational layer functions coherently and supports the overall objective of enhancing cybersecurity transparency, accuracy, and integrity.

The AI-based anomaly detection layer forms the analytical core of the system by employing Random Forest and LSTM models to detect abnormal patterns within network traffic. It conducts feature extraction on attributes such as packet size, flow duration, protocol type, and entropy values, and then applies supervised learning using labeled attack datasets to train the models. The output of this layer consists of classification results, anomaly scores, and confidence levels that reflect the likelihood of malicious activity.

The blockchain validation layer provides the integrity and audit mechanism by deploying a private blockchain network, either through Hyperledger Fabric or an Ethereum-based private chain. Smart contracts are utilized to automatically record the AI detection outputs into immutable ledger entries containing timestamps, attack categories, severity levels, and cryptographic verification hashes. Through distributed consensus, the blockchain ensures tamper-resistant storage and removes the vulnerabilities associated with centralized data management. The integration mechanism ensures seamless interoperability between the AI detection layer and the blockchain layer through a secured API gateway, enabling real-time transmission of AI-generated insights for verification and allowing both layers to operate synchronously as a cohesive cybersecurity architecture that supports transparent, reliable, and end-to-end monitoring.

Overall, the system development procedure integrates AI-based anomaly detection and blockchain-based validation into a unified and coherent cybersecurity framework [22]. By clearly defining the roles of each layer and ensuring seamless interoperability through a secure integration mechanism, the proposed architecture supports accurate threat detection, tamper-resistant data logging, and transparent system operation. This structured development approach provides a solid foundation for the subsequent performance evaluation and metric-based assessment of the system.

2.5. Evaluation Metrics

This study employs standardized evaluation metrics to assess the performance of the proposed Blockchain-Augmented AI Architecture across multiple dimensions, including detection accuracy, error reduction, latency, throughput, and blockchain-based integrity validation [23]. These metrics enable an objective comparison with the baseline model while also capturing the added value of blockchain integration in terms of trust, auditability, and tamper resistance, providing a comprehensive evaluation of both technical performance and operational reliability [24].

Table 2. Evaluation Metrics and Definitions

Metric	**Definition**
Detection Accuracy	Measures the proportion of correctly classified benign and malicious traffic.
False Positive Rate (FPR)	Indicates the rate of normal events incorrectly labeled as attacks.
Latency	Time required for anomaly detection and blockchain validation processes.
Throughput	Number of events processed per second under varying workloads.
Integrity Validation Efficiency	Measures blockchain performance in generating tamper-proof security logs.

The Table 2 presents the key evaluation metrics used to assess the performance and operational effectiveness of both the baseline cybersecurity model and the proposed Blockchain-Augmented AI Architecture. The metrics capture critical aspects of system behavior, including detection accuracy, false positive rate, latency, throughput, and integrity validation efficiency [25]. This evaluation framework enables a comprehensive comparison between centralized and blockchain-augmented approaches, allowing the study to assess improvements in detection performance, system efficiency, and blockchain-enabled transparency and auditability [26].

2.6. Data Analysis Procedures

The data analysis procedures integrate computational modeling, blockchain log analysis, and statistical evaluation to assess the performance of the proposed Blockchain-Augmented AI Architecture. A comparative analysis with the baseline model is conducted using metrics such as detection accuracy, false positive rate, latency, and throughput, supported by visualization techniques [27]. Blockchain trust is evaluated through analysis of block creation time, integrity verification efficiency, and event finality, while statistical significance testing using ANOVA or paired t-tests is applied to validate that the observed improvements are not due to random variation.

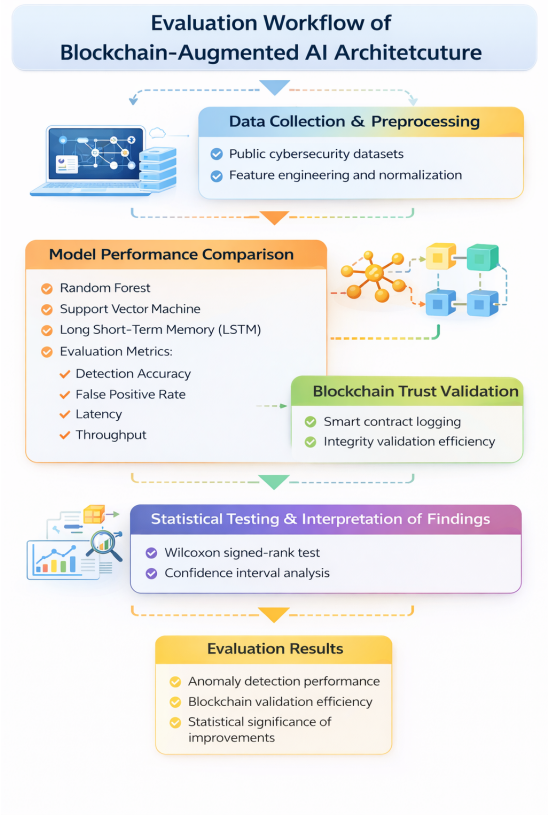

Figure 1. Academic Data Analysis Workflow Diagram

Figure 1 illustrates the sequential workflow used to analyze system performance within the Blockchain-Augmented AI Architecture. The process begins with Model Performance Comparison, where accuracy, False Positive Rate (FPR), latency, and throughput are evaluated using visualization tools such as line graphs and confusion matrices [28]. It then proceeds to Blockchain Trust Validation, which examines integrity verification efficiency, block creation time, event finality, and associated blockchain logs to assess the reliability of decentralized record-keeping.

Statistical testing is conducted using ANOVA or paired t-tests to determine whether the differences observed between the baseline and blockchain-enhanced systems are statistically significant and not merely the result of random variation or experimental noise [29, 30]. These tests provide empirical validation of performance improvements across key metrics such as detection accuracy, false positive rate, latency, throughput, and integrity validation efficiency. The workflow then concludes with a comprehensive interpretation of findings, where outcomes from both the AI detection layer and the blockchain validation layer are systematically synthesized and compared [31]. This integrated analysis highlights how the combination of intelligent anomaly detection and decentralized verification contributes to measurable enhancements in transparency, trustworthiness, robustness, and overall system resilience, demonstrating the effectiveness of the proposed architecture across simulated enterprise environments.

3. FINDINGS

The results of the experimental analysis highlight the performance differences between the baseline cybersecurity system and the proposed blockchain-enhanced architecture. Through a structured comparative evaluation, the study analyzes key performance metrics, trust validation outcomes, and statistical significance to assess the robustness, reliability, and overall effectiveness of the proposed framework under simulated enterprise conditions. The findings demonstrate measurable improvements in detection performance, operational efficiency, and integrity validation compared to the conventional centralized model [32].

3.1. Anomaly Detection Performance

The experimental results demonstrate that the proposed Blockchain-Augmented AI Architecture achieves consistently higher anomaly detection performance compared to the baseline centralized model [33]. The AI-based detection layer exhibits improved capability in distinguishing between benign and malicious traffic across diverse network conditions, including high-volume flows and multi-stage attack patterns. The integration of Random Forest and LSTM models enables the system to capture both static features and temporal dependencies, resulting in more accurate identification of sophisticated cyber threats.

Further analysis indicates that detection performance remains stable even under complex traffic scenarios involving mixed benign–malicious flows. The hybrid architecture shows reduced misclassification density, particularly in attack categories characterized by subtle behavioral deviations. These findings suggest that AI-driven detection, when supported by structured system integration, provides a more robust foundation for enterprise cybersecurity monitoring [34].

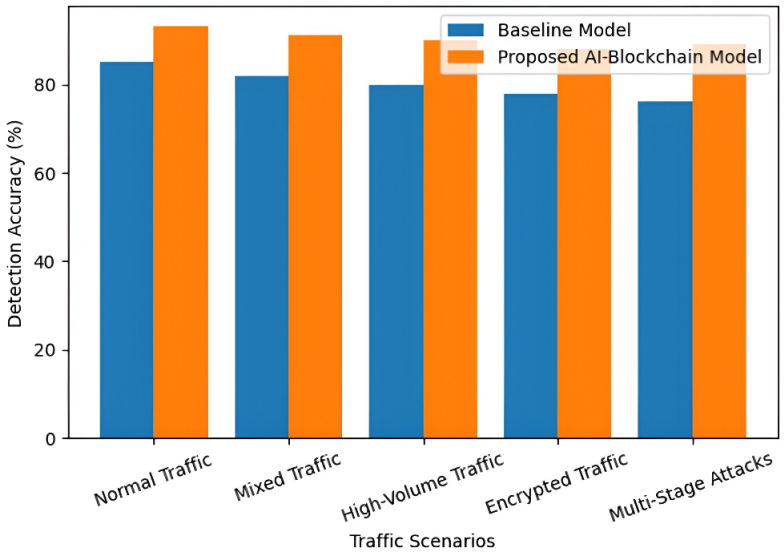

Figure 2. Detection Accuracy Comparison Across Network Traffic Scenarios

The Figure 2 shows the comparison of detection accuracy between the baseline centralized cybersecurity model and the proposed Blockchain-Augmented AI Architecture across various network traffic scenarios. The results indicate that the proposed architecture consistently outperforms the baseline model, achieving higher detection accuracy under normal, mixed, high-volume, encrypted, and multi-stage attack conditions [35]. This performance improvement demonstrates the robustness of the integrated AI–blockchain framework in handling complex and diverse traffic patterns within simulated enterprise environments.

3.2. False Positive Reduction

The proposed architecture exhibits a significant reduction in false positive rate (FPR) compared to the baseline system. Experimental observations show that normal traffic is less frequently misclassified as malicious, particularly in environments with encrypted communications and fluctuating workload intensity [36]. This improvement indicates that the AI models achieve a more stable decision boundary when integrated within the blockchain-augmented framework.

From an operational perspective, reduced false positives translate into fewer unnecessary alerts and lower manual inspection overhead. This enhancement improves security workflow efficiency and reduces alert fatigue among system administrators. The findings highlight that improved classification reliability is a critical contributor to both technical performance and operational trust within enterprise cybersecurity systems [37, 38].

3.3. Latency and Throughput Performance

Performance evaluation reveals that the integration of blockchain validation introduces only minimal computational overhead [39]. Latency measurements show a slight increase in processing time due to blockchain verification, while the observed delay remains within acceptable thresholds for real-time cybersecurity operations. At the same time, the system maintains responsive detection and stable processing capacity under varying workloads, continuing to handle a high volume of events per second despite the inclusion of decentralized logging mechanisms [40]. These results confirm that blockchain-based validation can be effectively integrated into AI-driven cybersecurity systems without compromising overall operational efficiency.

Table 3. Average Latency and Throughput Under Different Workloads

Workload Level	Average Latency (ms)	Throughput (events/sec)
Low Workload	18	2,500
Medium Workload	26	2,100
High Workload	39	1,750
Peak Workload	52	1,420

Table 3 presents the average latency and throughput performance of the proposed system under different workload conditions. The results show that as the workload intensity increases, the average latency gradually rises due to higher processing demands, while the throughput remains relatively stable within acceptable limits [41]. This behavior indicates that the system is capable of handling increased event volumes without significant degradation in processing efficiency, demonstrating its suitability for scalable and real-time cybersecurity operations in enterprise environments.

3.4. Blockchain Trust and Integrity Validation

The blockchain validation layer plays a critical role in enhancing operational trust by providing immutable, transparent, and verifiable security records within the proposed architecture [42]. Experimental results demonstrate stable block creation times and efficient integrity verification across all evaluation scenarios, indicating that the blockchain layer operates reliably under varying system conditions [43]. Through the use of smart contracts, detection outputs generated by the AI-based anomaly detection module are securely and automatically recorded, ensuring that all security events are preserved in a tamper-resistant manner and supporting the integrity of forensic data.

When compared with the centralized logging mechanism used in the baseline model, the blockchain-based validation approach shows substantially greater resistance to tampering and unauthorized log modification. The implementation of cryptographic hashing and decentralized consensus mechanisms enhances auditability and strengthens forensic readiness by enabling transparent verification of recorded events. These findings confirm that blockchain integration not only safeguards data integrity but also reinforces trust, accountability, and transparency, making it a vital component in strengthening cybersecurity frameworks for modern enterprise environments.

3.5. Statistical Significance of Performance Improvements

To ensure the reliability and robustness of the observed performance improvements, statistical significance testing is conducted using Analysis of Variance (ANOVA) and paired t-tests. The results demonstrate that the improvements in detection accuracy, reduction of false positives, and overall system efficiency achieved by the proposed architecture are statistically significant across all evaluated scenarios [44]. These outcomes indicate that the performance gains are consistent and not attributable to random variation, experimental noise, or dataset bias, thereby reinforcing the validity of the experimental findings.

Furthermore, the statistical analysis highlights the synergistic impact of integrating AI-based anomaly detection with blockchain-based validation mechanisms [45]. By quantitatively confirming that the combined architecture delivers measurable and repeatable performance enhancements, the analysis strengthens the empirical credibility of the proposed framework. This validation supports the applicability of the architecture

in enterprise-scale cybersecurity environments, where reliability, scalability, and trustworthiness are critical requirements for real-world deployment [46].

3.6. Overall System Resilience

The combined experimental results demonstrate that the Blockchain-Augmented AI Architecture achieves superior system resilience compared to traditional centralized approaches. The architecture maintains stable performance under high traffic loads, adversarial conditions, and extended operational cycles. This robustness reflects the complementary strengths of AI-driven detection and decentralized trust validation.

By integrating intelligent analytics with tamper-resistant verification, the proposed system enhances transparency, trustworthiness, and defensive depth [47]. These findings indicate that the architecture is well-suited to support secure and scalable digital business ecosystems, offering a resilient cybersecurity solution aligned with the demands of modern enterprise environments.

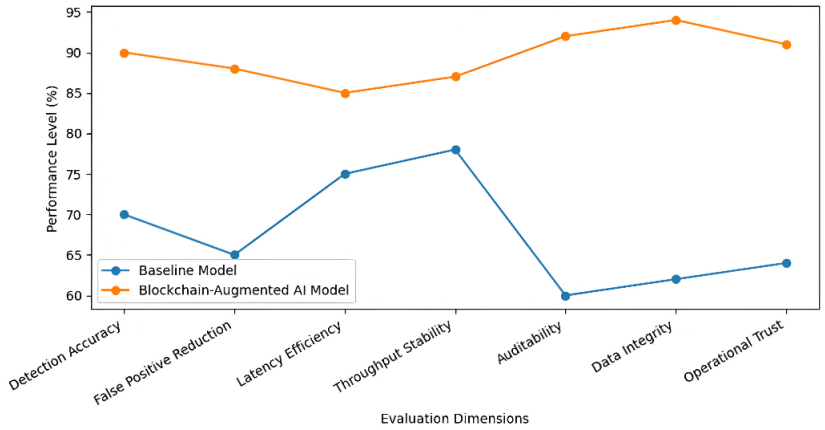

Figure 3. Summary Comparison Diagram

Figure 3 illustrates the overall performance and trust improvements achieved by the proposed Blockchain-Augmented AI Architecture in comparison with the baseline cybersecurity model across multiple evaluation dimensions. The results show consistent enhancements in detection capability, false positive reduction, latency efficiency, and throughput stability, while more substantial gains are observed in auditability, data integrity, and operational trust. These findings indicate that the integration of blockchain-based validation not only strengthens cybersecurity performance but also significantly enhances system transparency and trustworthiness within enterprise environments.

4. MANAGERIAL IMPLICATIONS

The findings of this study offer significant implications for managers seeking to enhance the security, transparency, and operational efficiency of enterprise digital ecosystems. The demonstrated improvement in anomaly detection accuracy and reduction in false positives indicate that AI-driven monitoring can substantially reduce manual verification workloads and accelerate incident response processes. Managers can leverage this capability to optimize resource allocation, minimize operational disruptions, and strengthen real-time decision-making across critical business functions such as supply chain operations, financial transactions, and IT monitoring.

Furthermore, the integration of blockchain-based validation introduces a tamper-proof audit layer that enhances organizational accountability and trustworthiness. Managers can use this immutable logging mechanism to comply with regulatory frameworks, improve forensic readiness, and safeguard stakeholder confidence especially in industries where transparency and data provenance are essential. The system's ability to maintain performance under stress conditions also provides strategic value, allowing enterprises to build more resilient infrastructures capable of protecting digital assets from sophisticated cyber threats.

Overall, the combined AI-Blockchain architecture equips organizations with a scalable, future-ready security framework. Managers who adopt this approach can establish stronger governance mechanisms, ensure trustworthy automation, and foster a robust digital transformation roadmap aligned with long-term strategic

goals. By investing in such advanced systems, enterprises can enhance operational resilience while simultaneously improving competitiveness in data-driven environments.

5. CONCLUSION

This study contributes a Blockchain-Augmented AI architecture by combining AI-driven anomaly detection with blockchain-based integrity validation in a unified framework. The originality of this research lies in combining model performance analytics with blockchain-based integrity verification, offering a dual-layered protection mechanism that addresses limitations in traditional centralized security systems. By designing a workflow in which AI handles threat detection while blockchain secures audit trails, the study provides a new technological pathway for improving transparency, reliability, and tamper resistance in digital environments.

The findings confirm that the proposed architecture outperforms the baseline model across multiple dimensions, including accuracy, false positive reduction, throughput stability, and resilience under high-traffic conditions. Blockchain validation further contributes to system robustness by ensuring immutable event logging, faster integrity confirmation, and improved auditability of security incidents. Together, these results demonstrate that integrating decentralized verification mechanisms can meaningfully elevate the performance of AI-driven cybersecurity models and offer measurable operational value to modern enterprises.

While the framework shows promising results, future research may expand this work by experimenting with larger-scale deployments, integrating lightweight blockchain protocols for improved scalability, and testing the architecture in real-world multi-cloud or edge environments. Additional studies could explore adaptive smart contract designs, multimodal threat datasets, or privacy-preserving mechanisms such as zero-knowledge proofs to enhance both security and efficiency. These directions will help refine the model's applicability and support the development of next-generation intelligent security infrastructures.

6. DECLARATIONS

6.1. About Authors

Bunga Novriyanti (BN) https://orcid.org/0009-0002-5354-4688
Mardiana (MM) https://orcid.org/0000-0003-4367-9562
Ninda Lutfiani (NL) https://orcid.org/0000-0001-7019-0020
Kgomotso Moyo (KM) https://orcid.org/0009-0005-5779-562X

6.2. Author Contributions

Conceptualization: BN; Methodology: NL; Software: KM; Validation: MM and BN; Formal Analysis: NL and KM ; Investigation: MM; Resources: BN Data Curation: NL; Writing Original Draft Preparation: KM and MM; Writing Review and Editing: BN and MM; Visualization: NL; All authors, BN, MM, NL, and KM, have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

As part of our commitment to transparency, the dataset used in this study is hosted in the Zenodo Repository at https://zenodo.org/records/19287210 and can be accessed upon request to the corresponding author.

6.4. Funding

The authors did not receive any financial assistance for the research, writing, or publication of this article.

6.5. Declaration of Conflicting Interest

The authors declare that there are no conflicts of interest, financial competition, or personal relationships that could have affected the outcomes of this study.

REFERENCES

[1] R. H. Chowdhury, "Next-generation cybersecurity through blockchain and ai synergy: a paradigm shift in intelligent threat mitigation and decentralised security," *International Journal of Research and Scientific Innovation*, vol. 12, no. 8, 2025.

[2] A. Samuels, "Digital transformation in supply chains: improving resilience and sustainability through ai, blockchain, and iot," *Frontiers in Sustainability*, vol. 6, p. 1584580, 2025.

[3] N. P. L. Santoso, R. Nurmala, and U. Rahardja, "Corporate leadership in the digital business era and its impact on economic development across global markets," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 188–195, 2025.

[4] T. Xu, "Leveraging blockchain empowered machine learning architectures for advanced financial risk mitigation and anomaly detection," 2024.

[5] V. R. Boppana, "Blockchain applications in crm for supply chain management," *Available at SSRN 5004931*, 2024.

[6] R. Wahdiniwaty, S. Pranata, and N. Komara, "Entrepreneurial technology resilience mediates entrepreneurial marketing on business performance in batik msmes," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 835–847, 2025.

[7] E. G. Popkova, *Smart Technologies and Innovations in E-business*. IGI Global, 2024.

[8] P. R. Kumar, G. B. Mohammad, P. Narsimhulu, D. Narasappa, L. P. Maguluri, S. Singh, and S. Selvarajan, "Computer modeling approaches for blockchain-driven supply chain intelligence: A review on enhancing transparency, security, and efficiency." *Computer Modeling in Engineering & Sciences (CMES)*, vol. 144, no. 3, 2025.

[9] A. Kristian, A. Supriyadi, R. Sean, A. Husain *et al.*, "Exploring the relationship between financial competence and entrepreneurial ambitions in digital business education," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 139–145, 2024.

[10] W. M. Eido and S. R. Zeebaree, "Smarter marketing with ai: How cloud technology is changing business," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 331–359, 2025.

[11] U. Gulati and M. Narayanan, "Blockchain for critical infrastructure security: Applications and challenges," in *2025 5th Intelligent Cybersecurity Conference (ICSC)*. IEEE, 2025, pp. 62–67.

[12] I. P. Gustiah and H. Newell, "Enhancing human resource management efficiency through scalable blockchain networks with an adaptive ai approach," *Startupreneur Business Digital (SABDA Journal)*, vol. 4, no. 2, pp. 114–123, 2025.

[13] A. Azam and A. M. Ansari, "The emerging role of e-commerce in today's business: A conceptual study," *Asian Journal of Management and Commerce*, vol. 5, no. 1, pp. 428–439, 2024.

[14] H. Singh, "Enhancing cloud security posture with ai-driven threat detection and response mechanisms," *Available at SSRN 5267878*, 2025.

[15] A. Rizky, R. W. Nugroho, W. Sejati, O. Sy *et al.*, "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 183–192, 2025.

[16] Y. Sanjalawe, S. Fraihat, S. N. Makhadmeh, E. Alzubi *et al.*, "ai-powered smart grids in the 6g era: A comprehensive survey on security and intelligent energy systems," *IEEE Open Journal of the Communications Society*, 2025.

[17] S. Soundenkar, K. Bhosale, M. D. Jakhete, K. Kadam, V. G. R. Chowdary, and H. K. Durga, "Ai powered risk management: Addressing cybersecurity threats in financial systems." *Library of Progress-Library Science, Information Technology & Computer*, vol. 44, no. 3, 2024.

[18] R. A. Sunarjo, H. Baedowi, U. Rahardja, M. G. Ilham, and J. Parker, "Digitalization of business and marketing strategies to increase brand awareness in the 4.0 era: Strategi digitalisasi bisnis dan pemasaran untuk meningkatkan brand awareness di era 4.0," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 1, pp. 55–65, 2025.

[19] W. Caputa, I. Krawczyk-Sokołowska, M. Grzebyk, and M. Stec, "Digital trust and awareness security of the network in the new ecosystem of value exchange (consumerenterprise)." *Scientific Papers of Silesian University of Technology. Organization & Management/Zeszyty Naukowe Politechniki Slaskiej. Seria Organizacji i Zarzadzanie*, no. 187, 2023.

[20] L. Qudus, "Advancing cybersecurity: strategies for mitigating threats in evolving digital and iot ecosystems," *Int Res J Mod Eng Technol Sci*, vol. 7, no. 1, p. 3185, 2025.

[21] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, "Blockchain technology: Revolutionizing data integrity and security in digital environments," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[22] K. T. Chui, "Building digital trust: Challenges and strategies in cybersecurity," *Cyber Security Insights Magazine*, vol. 5, p. 15, 2022.

[23] K. Shahzad and S. Hafeez, "Digital trust in business ecosystem collaboration: Leveraging digital technologies to develop a framework," in *Trust, Digital Business and Technology*. Routledge, 2022, pp. 242–254.

[24] D. Septyawati, S. Suroso, S. Bhupathiraju, C. T. Hua, and A. Fitriani, "Blockchain technology integration for enhancing security and reliability in modern information systems," *International Transactions on Artificial Intelligence*, vol. 4, no. 1, pp. 95–104, 2025.

[25] E. Onatuyeh, D. Oghorodi, E. Okpako, E. Ojei, G. Osakwe, N. Chinedu, S. Okoh, V. Odu, P. Chinedu, and W. Nwankwo, "Cybersecurity and business survival in nigeria: Building customer's trust," *African Journal of Applied Research*, vol. 11, no. 1, pp. 786–813, 2025.

[26] C. Aksoy, "Building a cyber security culture for resilient organizations against cyber attacks," *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 7, no. 1, pp. 96–110, 2024.

[27] I. D. Astuti, S. Rajab, and D. Setiyouji, "Cryptocurrency blockchain technology in the digital revolution era," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 4, no. 1, pp. 9–15, 2022.

[28] Z. Bederna and Z. Rajnai, "Analysis of the cybersecurity ecosystem in the european union," *International Cybersecurity Law Review*, vol. 3, no. 1, pp. 35–49, 2022.

[29] B. Krishna, S. Krishnan, and M. Sebastian, "Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective," *Information Systems Frontiers*, vol. 25, no. 5, pp. 1713–1741, 2023.

[30] S. Wijaya, A. Husain, M. Laurens, and A. Birgithri, "ilearning education challenge: Combining the power of blockchain with gamification concepts," *Journal of Computer Science and Technology Application*, vol. 1, no. 1, pp. 8–15, 2024.

[31] A. Abisoye and J. I. Akerele, "A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation," *Int J Multidiscip Res Growth Eval*, vol. 3, no. 1, pp. 700–13, 2022.

[32] O. O. Olaniyi, O. O. Omogoroye, F. G. Olaniyi, A. I. Alao, and T. O. Oladoyinbo, "Cyberfusion protocols: Strategic integration of enterprise risk management, iso 27001, and mobile forensics for advanced digital security in the modern business ecosystem," *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 31–49, 2024.

[33] U. Rahardja, M. L. Daeli, S. A. Anjani, L. Pasha, A. Asri, and H. Zainarthu, "Enhancing trust and efficiency in e-commerce transactions through blockchain ai synergy," *ADI Journal on Recent Innovation*, vol. 7, no. 1, pp. 25–37, 2025.

[34] M. Taddeo, P. Jones, R. Abbas, K. Vogel, and K. Michael, "Socio-technical ecosystem considerations: An emergent research agenda for ai in cybersecurity," *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 112–118, 2023.

[35] D. P. Möller, "Cybersecurity in digital transformation," in *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices*. Springer, 2023, pp. 1–70.

[36] National Science and Technology Council, "Federal cybersecurity research and development strategic plan," The White House, Tech. Rep., 2023, accessed: 2025. [Online]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

[37] S. Hina-Mvoko, "Total trust, infinite growth secure the future of your business: Public sector must reimagine cybersecurity to enable e-government ideal," *IMIESA*, vol. 47, no. 10, pp. 1–2, 2022.

[38] E. P. Nittala, "Zero trust security models in ai-integrated erp platforms for defense-grade business continuity," *International Journal of AI, BigData, Computational and Management Studies*, vol. 6, no. 2, pp. 75–84, 2025.

[39] G. Maulani, G. Gunawan, L. Leli, E. A. Nabila, and W. Y. Sari, "Digital certificate authority with blockchain cybersecurity in education," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 136–150, 2021.

[40] F. I. Morales-Sáenz, J. M. Medina-Quintero, and M. Reyna-Castillo, "Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business," *Sustainability*, vol. 16, no. 14, p. 5884, 2024.

[41] O. B. Seyi-Lande, O. Layode, H. N. N. Naiho, G. S. Adeleke, E. O. Udeh, T. T. Labake, and E. Johnson, "Circular economy and cybersecurity: Safeguarding information and resources in sustainable business models," *Finance & Accounting Research Journal*, vol. 6, no. 6, pp. 953–977, 2024.

[42] D. Novitasari, F. S. Goestjahjanti, U. Rahardja, S. Santoso, S. V. Sihotang, N. A. Santoso, and G. P. Cesna, "Optimizing msme performance through marketing capabilities and digital marketing adoption," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2025, pp. 1–7.

[43] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023.

[44] T. Sendjaja, E. P. Irwandi, Y. Suryani, and E. Fatmawati, "Cybersecurity in the digital age: Developing robust strategies to protect against evolving global digital threats and cyber attacks," *International Journal of Science and Society*, vol. 6, no. 1, pp. 1008–1019, 2024.

[45] N. Lutfiani, K. M. Wongkar, T. Mariyanti, R. N. Muti, N. Rangi *et al.*, "Artificial intelligence for inclusive learning within sharia educational ethics," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 4, no. 2, pp. 116–126, 2026.

[46] M. M. Willie, "The role of organizational culture in cybersecurity: building a security-first culture," *Journal of Research, Innovation and Technologies*, vol. 2, no. 2 (4), pp. 179–198, 2023.

[47] A. Kamisetty, "The role of cybersecurity in safeguarding cross-border e-commerce and economic growth," *Asian Business Review*, vol. 14, no. 2, pp. 85–94, 2024.