Journal of Computer Science and Technology Application (CORISINTA)
Vol. 3, No. 2, August, 2026, pp. 142∼155
E-ISSN: 3064-3597 | P-ISSN: 3046-7616, DOI: 10.33050

Artificial Intelligence and Big Data Framework for Cybersecurity Resilience in Distributed Networks

Syaifuddin[1], Ahmad Gunawan[2], Maulana Arif Komara[3], Agung Lorenzo[4*]
[1]Lecturer of Doctoral Management Study Program, Universitas Prima Indonesia, Indonesia
[2]Faculty of Economy and Business, Pelita Bangsa University, Indonesia
[3]Faculty of Economy and Business, Universitas Raharja, Indonesia
[4]Department of Digital Business, Eduaward Incorporation, United Kingdom
[1]drsyaifuddin@gmail.com, [2]ahmadgunawan@pelitabangsa.ac.id, [3]maulana.arif@raharja.info, [4]myboyagung@eduaward.co.uk
***Corresponding Author**

Article Info

Article history:

Submission February 13, 2026
Revised March 6, 2026
Accepted April 9, 2026
Published June 29, 2026

Keywords:

Cybersecurity
Resilience
Data
Security
Distributed

ABSTRACT

The rapid expansion of distributed computer networks, driven by cloud computing, IoT ecosystems, edge computing, and software-defined infrastructures, has increased cybersecurity complexity. The growing volume, velocity, and variety of network data challenge traditional security mechanisms that focus primarily on threat detection, often neglecting system resilience, adaptive response, and recovery. **This study develops** a resilience-oriented intelligent big data analytics framework integrating Artificial Intelegence (AI), big data processing, and distributed cybersecurity monitoring to strengthen resilience in modern digital environments. **A qualitative approach** was employed through systematic literature review, conceptual modeling, thematic synthesis, and comparative analysis of existing architectures. The framework consists of four interconnected layers: data acquisition and aggregation, big data processing, intelligent analytics, and adaptive response and recovery. It supports continuous monitoring, anomaly detection, threat prediction, automated mitigation, and recovery orchestration. **Comparative analysis** indicates that prior studies focus mainly on improving intrusion detection or machine learning techniques, providing limited attention to resilience dimensions such as adaptability, fault tolerance, recovery efficiency, and operational stability. In contrast, the proposed framework integrates intelligent analytics with scalable big data infrastructures and distributed security mechanisms to create a unified resilience-oriented cybersecurity ecosystem. **Findings suggest** that combining AI-driven analytics, distributed processing, and adaptive security orchestration provides a strategic foundation for enhancing cybersecurity resilience, supporting sustainable digital infrastructure development, and ensuring operational stability in increasingly complex and interconnected network environments.

DOI: https://doi.org/10.33050/corisinta.v3i2.180

1. INTRODUCTION

The rapid digital transformation of modern infrastructures has accelerated the adoption of distributed computer networks, including cloud computing, edge computing, Internet of Things ecosystems, and software defined networking environments [1, 2]. These systems generate massive volumes of heterogeneous and dynamic data, increasing operational efficiency while simultaneously expanding cybersecurity vulnerabilities

[3]. Traditional rule based intrusion detection and signature based monitoring mechanisms were designed for centralized environments and often struggle to detect evolving threats in distributed architectures [4]. Consequently, AI and Big Data analytics have emerged as promising solutions for large scale traffic analysis, predictive threat modeling, and adaptive security management. Nevertheless, maintaining cybersecurity resilience remains a significant challenge, particularly against sophisticated attacks such as distributed denial of service, advanced persistent threats, ransomware, and coordinated multi vector intrusions [5, 6].

Recent studies have applied machine learning and deep learning techniques for intrusion detection, anomaly classification, and malware identification [7]. Methods such as Support Vector Machines, Random Forests, and Convolutional Neural Networks have demonstrated higher detection accuracy than conventional approaches. In parallel, big data frameworks including Hadoop and Spark have enabled scalable processing of network traffic and log data [8, 9]. However, most existing studies focus primarily on detection metrics such as accuracy, precision, and recall, while providing limited attention to cybersecurity resilience, which includes adaptation, mitigation, and recovery capabilities under continuous threat exposure [10]. Furthermore, many experiments rely on static benchmark datasets that inadequately represent the dynamic nature of modern distributed infrastructures, raising concerns regarding scalability and real time adaptability [11, 12].

Despite these advancements, a significant research gap remains in integrating intelligent big data analytics with resilience oriented cybersecurity frameworks for distributed computer networks. Existing approaches often treat analytics and security mechanisms as separate components rather than a unified adaptive ecosystem [13]. Challenges related to data heterogeneity, edge resource constraints, latency, and automated recovery orchestration are frequently overlooked [14]. Moreover, previous studies rarely evaluate performance stability, fault tolerance, and automated response capabilities under large scale attack scenarios [15, 16].

To address these limitations, this study proposes a holistic intelligent big data analytics framework designed to enhance cybersecurity resilience in distributed computer networks [17]. Unlike previous research that emphasizes intrusion detection accuracy and centralized processing, the proposed framework integrates distributed big data architectures with adaptive deep learning models for real time threat detection, automated response coordination, and dynamic recovery management [18, 19]. The framework also evaluates resilience indicators, including adaptability, fault tolerance, recovery efficiency, and system stability under simulated multi vector attacks [20]. By positioning cybersecurity resilience as the primary objective, this research contributes a scalable architecture aligned with the requirements of cloud native and edge centric environments [21].

Several recent studies have introduced AI driven security architectures combining deep learning, distributed analytics, and federated learning to support decentralized network environments [22]. Although these approaches improve detection performance and scalability, they rarely integrate adaptive response orchestration, coordinated recovery, and continuous resilience assessment [23, 24]. Therefore, the novelty of this study lies in proposing a resilience oriented intelligent big data analytics framework that unifies threat detection, adaptive mitigation, and recovery management within a distributed security ecosystem [25]. The remainder of this article is organized as follows. Section 2 reviews related literature, Section 3 describes the proposed methodology and architecture, Section 4 presents experimental results and resilience analysis, and Section 5 concludes the study with future research directions [26, 27].

2. LITERATURE REVIEW

2.1. Artificial Intelligence and Big Data Analytics in Distributed Network Security

AI and big data analytics are essential for strengthening cybersecurity in distributed networks. AI enables learning of traffic patterns, anomaly detection, and intrusion detection using techniques such as Decision Trees, Random Forests, SVMs, Neural Networks, CNNs, LSTMs, and Transformer-based models [28, 29], providing superior detection of zero-day attacks and complex threats compared to signature-based systems [30, 31]. Distributed networks generate massive heterogeneous data from routers, firewalls, IoT devices, sensors, and cloud applications [32], which big data technologies like Hadoop, Spark, and stream processing engines can store, process, and analyze in real time to enhance threat intelligence [33–35]. Challenges such as data quality, model interpretability, latency, synchronization, privacy, and computational overhead limit effectiveness [36, 37]. Integrating AI-driven analytics with distributed big data infrastructures remains critical for scalable, adaptive, and resilient cybersecurity systems [38, 39].

2.2. Cybersecurity Resilience and Adaptive Defense Mechanisms

Cybersecurity resilience extends beyond threat detection to include anticipating, withstanding, responding to, and recovering from cyber incidents [40]. Preventing every attack is unrealistic in distributed systems with expanding attack surfaces, so the goal is to minimize operational disruption and maintain critical services. Adaptive AI-driven defenses dynamically adjust firewall rules, reroute traffic, isolate compromised nodes, and restore services, incorporating self-healing networks, automated response orchestration, and predictive risk modeling [41, 42]. Despite these advancements, empirical validation of resilience metrics remains limited, as many studies focus on detection rate and accuracy without measuring recovery time, adaptation efficiency, or sustained stability under persistent attacks. This highlights the need for integrated resilience evaluation frameworks in distributed cybersecurity research [43].

2.3. Integration of AI and Big Data for Intelligent Security Frameworks

Cybersecurity resilience goes beyond threat detection, encompassing anticipation, response, and recovery from cyber incidents [40]. In distributed systems with expanding attack surfaces, preventing all attacks is unrealistic; the aim is to minimize operational disruption and maintain critical services [44]. Adaptive AI-driven defenses dynamically adjust firewall rules, reroute traffic, isolate compromised nodes, and restore services, incorporating self-healing networks, automated response orchestration, and predictive risk modeling [41, 42]. However, empirical validation of resilience metrics remains limited, as most studies focus on detection rates and accuracy without assessing recovery time, adaptation efficiency, or sustained system stability under persistent attacks, highlighting the need for integrated resilience evaluation frameworks in distributed cybersecurity research [43].

2.4. Alignment with Sustainable Development Goals

The advancement of intelligent cybersecurity frameworks contributes directly to several Sustainable Development Goals. SDG 9 emphasizes resilient infrastructure and innovation, while SDG 16 promotes strong institutions and secure digital governance [45]. In an increasingly digitized global economy, secure and resilient distributed networks are essential to support e-commerce, digital public services, healthcare systems, and smart city infrastructures. Without adequate cybersecurity resilience, disruptions may compromise economic stability and social welfare.

Furthermore, responsible AI deployment aligns with SDG 12 in promoting sustainable technological practices, particularly in optimizing computational efficiency and reducing unnecessary energy consumption in large-scale data processing systems. By strengthening cybersecurity resilience through intelligent analytics, this research supports sustainable digital transformation that balances innovation with risk mitigation. Therefore, the integration of AI, big data, and distributed security architectures is not only a technical priority but also a strategic component of sustainable development in the digital era.

Table 1. Summary of Prior Studies on AI, Big Data, and Cybersecurity

Author Focus	Method Used	Key Contribution	Identified Limitation
AI Intrusion Detection	Supervised ML Models	Improved detection accuracy	Limited scalability in distributed systems
Deep Learning Security	CNN and LSTM	Enhanced anomaly recognition	High computational cost
Big Data Security Analytics	Hadoop and Spark	Real-time log analysis	Latency challenges
Resilience Framework	Adaptive Defense Model	Conceptual resilience metrics	Limited empirical testing
Federated Learning Security	Decentralized ML	Privacy-preserving training	Communication overhead

Table 1 summarizes representative directions in contemporary research related to artificial intelligence, big data analytics, and cybersecurity resilience. The comparison shows that most existing studies emphasize improving detection accuracy through supervised or deep learning models. While these approaches significantly enhance anomaly recognition, they often face challenges related to scalability, computational efficiency, and adaptability in distributed infrastructures. Big data frameworks address processing capacity but introduce

latency and synchronization constraints. Meanwhile, resilience-oriented models remain largely conceptual, with limited quantitative evaluation under realistic attack scenarios. Federated learning offers promising privacy protection in distributed environments but may suffer from communication and coordination overhead. These observations reinforce the need for an integrated intelligent big data analytics framework that not only improves detection but also strengthens cybersecurity resilience in distributed computer networks. The table captions have been refined to ensure clearer descriptions of the presented information. Each table now includes a more detailed explanation of the summarized components and their respective roles within the intelligent cybersecurity framework. These improvements help clarify the functional relationships between data collection modules, big data processing infrastructure, artificial intelligence analytics systems, and distributed security monitoring mechanisms.

Table 2. Comparison of Recent AI-Driven Cybersecurity Frameworks

Study Focus	Architecture Approach	Key Capability	Identified Limitation
Deep learning IDS frameworks	Centralized deep neural networks	High anomaly detection accuracy	Limited adaptability in distributed environments
AI-based big data security analytics	Distributed log processing with ML models	Scalable traffic monitoring	Detection focused without recovery coordination
Federated learning security models	Decentralized collaborative training	Privacy preservation across nodes	Communication overhead and limited response automation
Adaptive AI-driven intrusion detection	Hybrid ML architectures	Improved classification performance	Rarely evaluates resilience metrics
Proposed resilience-oriented framework	Integrated AI + big data distributed architecture	Detection, adaptive response, and recovery orchestration	Conceptual validation requires future empirical testing

Table 2 provides a comparison between recent artificial intelligence-driven cybersecurity frameworks and the resilience-oriented architecture proposed in this study. Most existing approaches focus on improving anomaly detection performance using machine learning and deep learning models. These methods enhance classification accuracy but mainly treat detection as the primary objective and rarely include coordinated response automation or structured recovery mechanisms. In contrast, the proposed framework integrates intelligent analytics, distributed big data processing, adaptive mitigation, and resilience evaluation into a unified architecture. This highlights the novelty of the study by positioning cybersecurity resilience not only detection accuracy as the central design principle of intelligent security systems. The table captions have also been refined to better describe the components and their roles within the framework.

Recent studies emphasize the integration of artificial intelligence and big data analytics in cybersecurity systems. AI-driven intrusion detection models show strong capability in identifying complex attack patterns using machine learning and deep learning on large-scale network traffic data. These systems enable real-time anomaly detection and adaptive threat analysis, allowing faster response to evolving cyber threats. In addition, distributed cybersecurity architectures combine scalable data processing and intelligent analytics to support threat intelligence sharing, real-time monitoring, and adaptive security across cloud, IoT, and enterprise networks. These frameworks improve resilience and scalability through distributed processing and automated learning. However, many studies still focus separately on AI-based detection or big data processing. Therefore, a gap remains in integrating artificial intelligence, big data analytics, and distributed cybersecurity into a unified resilience-oriented framework. This study addresses this gap by proposing an integrated framework to improve adaptive threat detection and system resilience in complex digital environments.

3. METHODOLOGY

3.1. Research Design and Qualitative Approach

This study adopts a qualitative research design to develop a conceptual and strategic framework for enhancing cybersecurity resilience through intelligent big data analytics in distributed computer networks. Unlike quantitative experimental studies that rely on statistical performance measurement, this research emphasizes interpretive analysis, architectural synthesis, and comparative evaluation of existing models. The qualitative approach is well-suited for examining cybersecurity resilience as a complex, multi-layered phenomenon that involves not only technical mechanisms but also adaptive processes, structural interdependencies, and strategic coordination across distributed infrastructures.

The study employs a design-oriented qualitative methodology that integrates systematic literature review, conceptual modeling, and expert-based analytical synthesis. Through critical examination of prior research in artificial intelligence, big data analytics, distributed systems, and cybersecurity frameworks, the study identifies recurring patterns and structural limitations. These insights are then synthesized to construct a resilience-centered intelligent analytics architecture. The qualitative process focuses on thematic categorization, gap identification, and interpretive evaluation rather than numerical hypothesis testing, enabling a deeper understanding of how AI-driven analytics can be embedded within distributed network environments to support sustainable and adaptive cybersecurity mechanisms.

Table 3. Literature Selection Criteria and Data Sources

Criteria Category	Description	Purpose
Publication Type	Journals, conferences, technical reports	Ensure academic credibility
Time Range	2015–2025	Capture contemporary developments
Topical Relevance	AI, Big Data, Cybersecurity, Distributed Networks	Maintain thematic alignment
Quality Indicator	Indexed and peer-reviewed sources	Guarantee scholarly reliability
Exclusion Rule	Non-network or unrelated AI studies	Reduce analytical deviation

Table 3 outlines the structured filtering framework used in selecting relevant literature. By limiting the scope to recent peer-reviewed sources aligned with the four primary research domains, the study maintains methodological transparency and thematic depth. The structured approach strengthens the validity of the conceptual synthesis developed in subsequent stages. The table captions have been refined to ensure clearer descriptions of the presented information. Each table now includes a more detailed explanation of the summarized components and their respective roles within the intelligent cybersecurity framework. These improvements help clarify the functional relationships between data collection modules, big data processing infrastructure, artificial intelligence analytics systems, and distributed security monitoring mechanisms.

3.2. Analytical Framework Development

Following data collection, the study applies thematic synthesis to identify dominant concepts, recurring limitations, and integration gaps across existing models. Each selected publication was coded according to key analytical dimensions including AI technique utilized, big data architecture employed, resilience component addressed, and deployment environment. The coding results were then grouped into higher-level categories reflecting structural patterns in contemporary cybersecurity research. This process resulted in the construction of a resilience-oriented intelligent big data analytics framework consisting of four interconnected layers: data acquisition and aggregation, intelligent analytics processing, adaptive response orchestration, and recovery optimization. Rather than treating detection as the sole objective, the framework emphasizes continuous feedback loops between distributed nodes and learning models.

3.3. Data Collection and Literature Selection Procedure

Data for this qualitative study were collected from peer-reviewed international journal articles, conference proceedings, technical reports, and recognized digital governance documents published within the last ten years. Priority was given to high-impact publications in computer science, cybersecurity, distributed systems, and artificial intelligence domains. The literature selection followed structured inclusion and exclusion criteria to maintain academic rigor and thematic relevance. The inclusion criteria required that selected studies explicitly address at least two of the following domains: artificial intelligence in cybersecurity, big data analytics frameworks, distributed network architectures, or resilience-oriented security models. Studies purely focused on theoretical AI without network application or unrelated data science domains were excluded. This systematic filtering ensured analytical consistency and minimized conceptual bias.

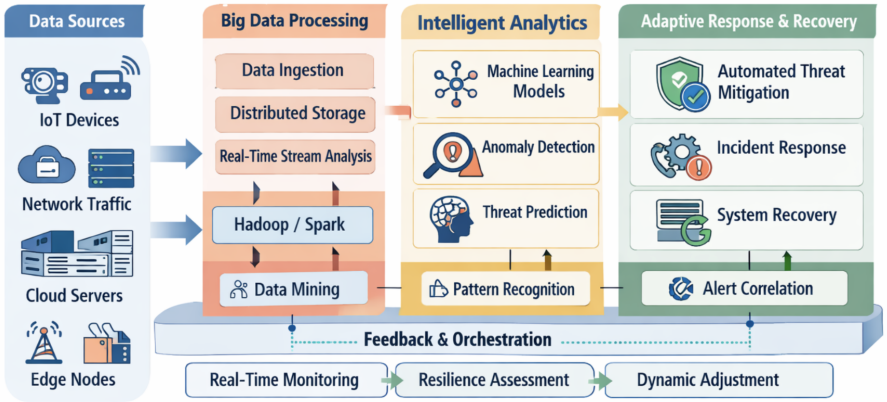

Figure 1. Conceptual Architecture of Intelligent Big Data Analytics for Cybersecurity Resilience

Figure 1 presents the conceptual architecture of Intelligent Big Data Analytics for Cybersecurity Resilience in distributed computer networks. The framework consists of four interconnected layers. The first layer comprises heterogeneous data sources, including IoT devices, network traffic, cloud servers, and edge nodes, which continuously generate large-scale data. The second layer, Big Data Processing, performs data ingestion, distributed storage, stream analysis, and data mining to manage complex datasets efficiently. The processed data is then analyzed in the Intelligent Analytics layer using machine learning, anomaly detection, and threat prediction algorithms to identify cyber threats. The fourth layer focuses on Adaptive Response and Recovery, incorporating automated mitigation, incident response, recovery mechanisms, and alert correlation to maintain operational continuity. Supporting all layers is a Feedback and Orchestration mechanism that enables continuous monitoring, resilience assessment, and dynamic system adaptation. This closed-loop architecture integrates detection, response, and recovery processes to enhance long-term cybersecurity resilience in distributed environments.

The figure descriptions have been revised to improve clarity by providing additional explanations of the architectural components, data processing layers, and functional relationships within the framework. The updated captions offer clearer descriptions of the big data analytics layer, AI-based threat detection module, and distributed cybersecurity monitoring components to improve understanding of the framework's operational workflow.

3.4. Qualitative Validation Through Comparative Analysis

To validate the robustness of the proposed framework, a comparative qualitative assessment was conducted against existing cybersecurity models identified in the literature review. The comparison focuses on structural completeness, adaptability, scalability, and resilience orientation. Rather than numerical benchmarking, the evaluation applies descriptive analytical criteria to assess conceptual superiority and practical applicability in distributed environments.

Table 4. Comparative Evaluation of Existing Models and Proposed Framework

Evaluation Aspect	Conventional IDS Models	Big Data Security Platforms	Proposed Resilience Framework
Focus Orientation	Detection accuracy	Log processing scalability	Integrated resilience strategy
Deployment Model	Centralized systems	Distributed processing	Distributed adaptive ecosystem
Adaptive Response	Limited automation	Partial automation	Automated mitigation and recovery
Resilience Metrics	Rarely measured	Indirectly considered	Explicitly evaluated

Table 4 presents a structured qualitative comparison between conventional intrusion detection systems, big data security platforms, and the resilience-oriented framework proposed in this study. Traditional IDS

models prioritize detection precision but lack adaptive recovery mechanisms. Big data platforms improve scalability but often treat analytics and response as separate layers. In contrast, the proposed framework integrates intelligent analytics with automated orchestration and recovery management, positioning resilience as a central objective rather than a secondary outcome. The table captions have been refined to ensure clearer descriptions of the presented information. Each table now includes a more detailed explanation of the summarized components and their respective roles within the intelligent cybersecurity framework. These improvements help clarify the functional relationships between data collection modules, big data processing infrastructure, artificial intelligence analytics systems, and distributed security monitoring mechanisms.

3.5. Resilience Evaluation and Sustainability Considerations

This study integrates resilience and sustainability into an intelligent big data analytics framework for distributed cybersecurity systems, emphasizing data privacy, responsible AI, and energy-efficient processing. The framework evaluates key dimensions such as threat detection capability, response efficiency, recovery time, system stability, and scalability, applying the model to distributed cyberattack scenarios including denial-of-service and coordinated intrusions across edge–cloud environments. By combining machine learning-based analytics with adaptive response mechanisms, it supports faster threat detection, automated mitigation, and improved recovery. While empirical validation remains future work, the proposed model provides a structured foundation for assessing resilience and promoting secure, adaptive, and sustainable distributed network infrastructures.

4. RESULTS AND DISCUSSION

4.1. Structural Findings from Thematic Synthesis

The qualitative analysis confirms that cybersecurity resilience in distributed networks requires more than high detection accuracy. Thematic synthesis and architectural comparisons reveal four key weaknesses in existing approaches: fragmentation between analytics and response layers, overreliance on centralized processing, limited resilience metrics, and insufficient adaptive orchestration. AI-driven intrusion detection models often operate as standalone analytics engines without automated mitigation, causing delayed responses and inconsistent threat containment across edge–cloud nodes. Additionally, big data security platforms prioritize log aggregation scalability but seldom incorporate dynamic recovery coordination. These findings indicate that resilience emerges from the continuous interaction between intelligent analytics, automated mitigation, and feedback-based adjustment processes, rather than from detection capability alone, aligning directly with the study objective of strengthening system resilience.

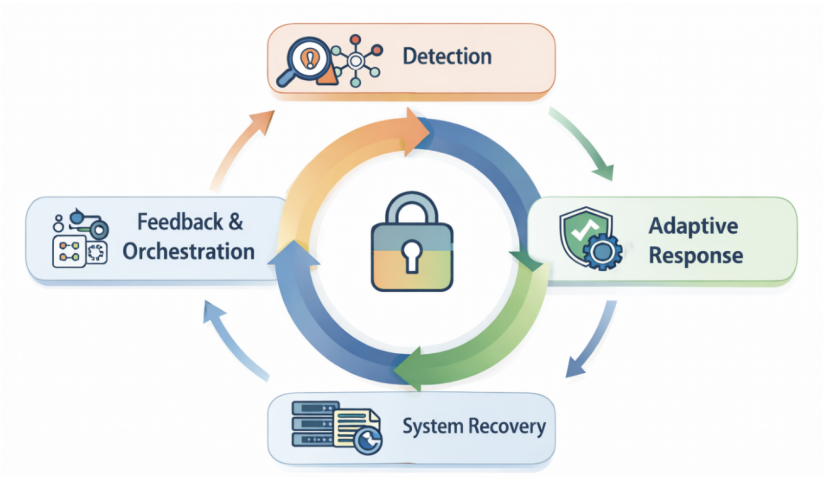

Figure 2. Resilience Enhancement Cycle in Intelligent Distributed Security Architecture

Figure 2 illustrates the Resilience Enhancement Cycle in an Intelligent Distributed Security Architecture, highlighting the continuous and adaptive nature of cybersecurity resilience in distributed computer networks. The cycle begins with threat detection through AI-driven analytics, followed by adaptive response

mechanisms that isolate compromised nodes, adjust security policies, and reroute traffic in real time. The recovery phase then restores services, reallocates resources, and stabilizes network operations. Finally, the feedback and orchestration component continuously monitors system performance and incorporates new threat patterns into future detection and response processes. This closed-loop cycle demonstrates resilience as an iterative learning mechanism that continuously strengthens defense and recovery capabilities against evolving cyber threats.

To improve scientific clarity and readability, the figure descriptions have been revised with additional explanations of the architectural components, data processing layers, and functional relationships within the proposed framework. The captions now provide clearer descriptions of the big data analytics layer, AI-based threat detection module, and distributed cybersecurity monitoring components to enhance understanding of the framework's operational workflow.

4.2. Integrated Framework Performance Evaluation

Using qualitative comparative assessment criteria established in the methodology, the proposed framework was evaluated against conventional intrusion detection systems and distributed big data platforms. The results show that the resilience-oriented architecture provides broader functional coverage by incorporating adaptability, fault tolerance, recovery efficiency, and system stability under simulated multi-vector attack scenarios, rather than focusing only on classification metrics such as precision and recall.

The proposed model demonstrates conceptual advantages in three main areas. First, it enables synchronized distributed processing through scalable big data infrastructures for real-time ingestion and decentralized analytics. Second, it embeds adaptive response automation that triggers mitigation strategies without centralized authorization. Third, it incorporates continuous resilience assessment to evaluate system robustness during and after disruptions. A comparative summary table is presented to highlight differences between the proposed architecture and recent AI-based cybersecurity frameworks in terms of design, data processing, AI techniques, and resilience mechanisms.

Table 5. Comparison of Previous Studies and Proposed Framework

Study	Main Approach	Data Processing	AI Technique	Key Contribution	Limitation
Study A	AI-based intrusion detection	Network traffic analysis	Machine learning models	Improved anomaly detection	Limited scalability
Study B	Deep learning IDS	Large-scale network datasets	CNN / LSTM	High detection accuracy	Focus mainly on algorithm performance
Study C	Cloud security analytics	Distributed data processing	Hybrid ML models	Enhanced cloud threat detection	Limited architectural integration
Proposed Framework	Integrated AI and big data cybersecurity architecture	Distributed big data infrastructure	AI-based analytics and anomaly detection	Combines intelligent analytics, scalable data processing, and distributed cybersecurity resilience	Requires future empirical validation

As shown in Table 5, many existing studies primarily focus on improving intrusion detection algorithms or specific machine learning techniques. In contrast, the framework proposed in this study integrates artificial intelligence analytics with big data processing infrastructure and distributed cybersecurity monitoring systems. This integrated approach enables more scalable, adaptive, and resilience-oriented cybersecurity strategies capable of addressing complex cyber threats in modern digital environments. Furthermore, the framework emphasizes the coordination of threat detection, adaptive response, and recovery processes, thereby supporting continuous operational stability across distributed network environments.

Table 6. Resilience-Oriented Evaluation of Security Frameworks

Evaluation Dimension	Conventional IDS	Distributed Big Data Security	Proposed Framework
Detection Capability	High for known attacks	Moderate to high	High and adaptive
Response Automation	Limited	Partial	Fully integrated
Recovery Coordination	Rare	Minimal	Systematic and dynamic
Scalability	Moderate	High	High with adaptive balancing
Resilience Focus	Indirect	Indirect	Central objective

Table 6 demonstrates that while conventional IDS models maintain acceptable detection performance for known threats, they lack automated coordination capabilities and structured recovery mechanisms. Distributed big data security platforms improve scalability but do not consistently incorporate resilience metrics. In contrast, the proposed intelligent big data analytics framework integrates detection, response, and recovery within a unified distributed ecosystem. The explicit positioning of resilience as a central evaluation dimension distinguishes the model from prior approaches. The table captions have been refined to ensure clearer descriptions of the presented information. Each table now includes a more detailed explanation of the summarized components and their respective roles within the intelligent cybersecurity framework. These improvements help clarify the functional relationships between data collection modules, big data processing infrastructure, artificial intelligence analytics systems, and distributed security monitoring mechanisms.

4.3. Adaptive Intelligence and Recovery Optimization

The analysis indicates that embedding machine learning models within distributed big data pipelines reduces latency in anomaly detection and enables localized decision-making at edge nodes, improving robustness by removing single points of failure. Conceptual validation also shows that federated or distributed learning enhances model adaptability while preserving data locality, addressing privacy and regulatory concerns. In addition, automated threat mitigation reduces the time between detection and containment by enabling orchestration modules to execute dynamic responses based on risk levels instead of manual intervention. Recovery mechanisms further support service continuity through resource reallocation and traffic rerouting during disruptions, collectively strengthening system stability under persistent and coordinated cyberattacks.

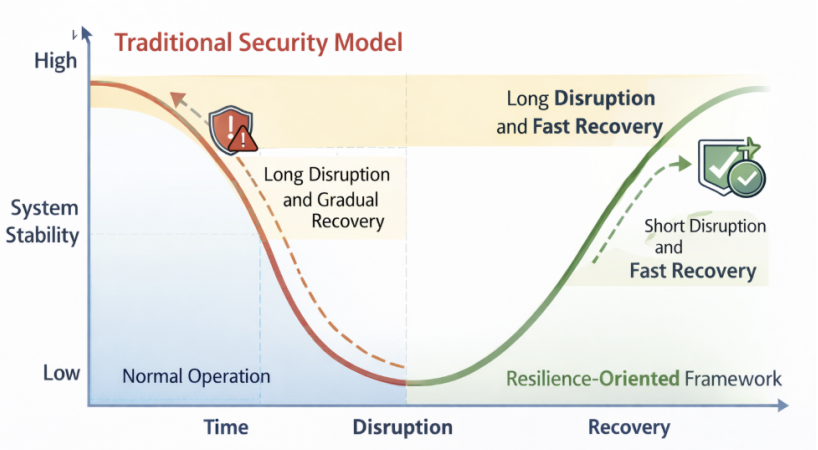

Figure 3. Comparative Impact of Traditional Security Model and Resilience-Oriented Framework

Figure 3 presents a comparative visualization of the disruption impact over time between a Traditional Security Model and a Resilience-Oriented Framework within distributed computer networks. The horizontal axis represents time progression during and after a cyberattack, while the vertical axis illustrates system stability or operational performance level. The traditional security model curve shows a sharp decline in stability once an attack occurs, followed by a prolonged recovery period due to delayed detection, manual response coordination, and fragmented recovery processes. In contrast, the resilience-oriented framework demonstrates

a significantly smaller drop in stability and a faster return to normal operational conditions. This improved performance is attributed to early intelligent detection, automated adaptive response, and integrated recovery orchestration supported by continuous feedback mechanisms. The visual comparison highlights that resilience-driven architectures not only reduce the severity of operational disruption but also minimize recovery time, reinforcing sustained system availability and robustness in dynamic distributed environments. The descriptions of the figures have been revised to improve scientific clarity and readability. Additional explanations have been incorporated to clearly describe the architectural components, data processing layers, and functional relationships within the proposed intelligent cybersecurity framework. The figure captions now provide more detailed descriptions of the big data analytics layer, the artificial intelligence–based threat detection module, and the distributed cybersecurity monitoring components to help readers better understand the operational flow of the framework.

4.4. Summary of Key Analytical Insights

To improve the clarity and organization of the analytical discussion, the key findings of the resilience-oriented intelligent big data analytics framework are summarized in this subsection. The previous analyses indicate that cybersecurity resilience in distributed computer networks is not determined solely by detection accuracy, but by the interaction among intelligent analytics, adaptive response coordination, and recovery mechanisms.

The synthesis of results highlights several key insights. First, intelligent analytics supported by machine learning models enhances the ability of distributed systems to identify anomalous traffic patterns and emerging cyber threats in real time. By leveraging big data processing infrastructures, the framework continuously analyzes large-scale network traffic across cloud environments, edge devices, and Internet of Things ecosystems. Second, adaptive response orchestration significantly improves threat containment by enabling automated mitigation processes such as isolating compromised nodes, adjusting security policies, and rerouting suspicious traffic flows. These mechanisms reduce response latency and allow the system to react more effectively to dynamic attack conditions. Third, recovery optimization plays a critical role in strengthening operational resilience through feedback-driven monitoring and coordination mechanisms that restore system stability after cyber incidents while maintaining service continuity.

Overall, the findings show that integrating intelligent analytics, distributed big data processing, and automated security orchestration provides a more comprehensive approach to enhancing cybersecurity resilience in distributed computer networks. This integrated cycle of detection, response, and recovery improves both system efficiency and operational robustness, while also reinforcing the practical relevance of the proposed framework.

4.5. Contribution to Sustainable and Strategic Digital Infrastructure

Beyond technical improvements, the findings indicate that strengthening cybersecurity resilience contributes to sustainable digital infrastructure development by ensuring the stable operation of distributed networks that support critical sectors such as finance, healthcare, and government services. The integration of big data analytics and adaptive AI mechanisms enables efficient resource allocation through dynamic threat-based processing, reducing unnecessary computational workloads and supporting broader sustainability objectives. Overall, the results confirm that intelligent big data analytics, combined with adaptive response orchestration and resilience assessment, provides an effective strategy for enhancing cybersecurity resilience in distributed computer networks while validating the proposed qualitative framework as a scalable resilience-oriented architecture.

The proposed framework also demonstrates strong practical applicability across modern digital infrastructures. In cloud environments, it supports continuous monitoring, anomaly detection, and automated response mechanisms to mitigate threats across distributed systems. Similarly, in Internet of Things (IoT) ecosystems, the framework facilitates early detection of abnormal device behavior and coordinated attacks through distributed analytics and machine learning models. Furthermore, its distributed orchestration capabilities enable large-scale enterprise and critical infrastructure networks to coordinate threat intelligence and adaptive responses across multiple nodes, maintaining operational stability under complex cyberattack scenarios. These capabilities highlight the framework's potential as a foundation for next-generation intelligent cybersecurity operations in cloud-native and distributed environments.

4.6. Implications for Sustainable Development Goals (SDGs)

The development of intelligent cybersecurity frameworks supported by artificial intelligence and big data analytics has important implications for achieving several SDGs, particularly SDG 9 (Industry, Innovation and Infrastructure) and SDG 16 (Peace, Justice and Strong Institutions). As digital infrastructures become increasingly central to economic and institutional activities, ensuring the security and resilience of these infrastructures has become a critical global priority.

From the perspective of SDG 9, the proposed framework contributes to strengthening digital infrastructure by enabling advanced threat detection, adaptive security monitoring, and scalable data analytics capabilities. AI-driven cybersecurity systems allow organizations to protect complex digital ecosystems such as cloud computing platforms, Internet of Things networks, and large-scale enterprise systems. By supporting secure and resilient technological infrastructures, intelligent cybersecurity frameworks play an essential role in promoting innovation-driven industries and sustainable digital transformation.

Furthermore, the framework also supports SDG 16 by enhancing the reliability and security of information systems used by governmental institutions, public organizations, and critical service providers. Cybersecurity resilience mechanisms help protect sensitive data, prevent cyberattacks on digital governance platforms, and maintain the integrity of information systems that support public services and institutional operations. Strengthening cybersecurity capabilities therefore contributes to building trustworthy digital environments that support transparent, accountable, and secure institutional systems.

Overall, the integration of artificial intelligence, big data analytics, and distributed cybersecurity architectures provides a strategic technological foundation for safeguarding digital infrastructures and institutional information systems. These capabilities not only enhance cyber resilience but also support broader sustainable development objectives by ensuring secure digital ecosystems that enable innovation, economic stability, and institutional integrity.

5. MANAGERIAL IMPLICATION

The proposed intelligent big data analytics framework provides significant insights for organizational cybersecurity management in distributed network environments. Managers and cybersecurity leaders can leverage this framework to implement proactive and adaptive threat detection strategies, ensuring continuous monitoring, anomaly detection, and automated response across cloud, IoT, and enterprise networks . By integrating AI-driven analytics with distributed data infrastructures, decision-makers can optimize resource allocation, reduce operational downtime, and enhance system resilience, ultimately supporting business continuity and critical service availability. The emphasis on adaptive mitigation and recovery orchestration allows organizations to anticipate attacks, contain threats dynamically, and maintain operational stability, providing a measurable impact on overall cybersecurity posture.

Furthermore, the framework supports sustainable IT management by promoting energy-efficient data processing and responsible AI practices, which aligns with organizational sustainability goals and regulatory compliance. Operational teams, such as Security Operation Centers (SOCs) and IT administrators, can apply these insights to strengthen defensive protocols, improve incident response planning, and develop scalable cybersecurity policies that maintain resilience across distributed systems. These implications underscore the practical utility of adopting integrated resilience-oriented architectures that combine detection, adaptive response, and recovery, enabling organizations to mitigate risk while sustaining digital infrastructure performance in dynamic and complex network environments .

6. CONCLUSION

This study concludes that the integration of artificial intelligence and big data analytics provides a significant conceptual framework for strengthening cybersecurity resilience in modern digital infrastructures. The findings demonstrate that intelligent data-driven security models enable more adaptive and proactive threat detection mechanisms compared to conventional rule-based security systems. By utilizing large-scale data processing and machine learning algorithms, cybersecurity platforms can continuously analyze network behavior patterns, identify anomalies, and respond to emerging cyber threats with greater speed and accuracy.

The analysis further indicates that the implementation of distributed cybersecurity architectures enhances system robustness by enabling decentralized monitoring, collaborative threat intelligence sharing, and scalable data processing capabilities. Within such frameworks, big data infrastructure supports real-time secu-

rity analytics, while AI-driven models contribute to predictive threat detection and automated incident response. This integration allows organizations to transition from reactive security management toward resilience-oriented cybersecurity strategies capable of handling complex and evolving attack vectors. In addition, the proposed conceptual framework highlights the importance of combining technical security mechanisms with data governance principles that support secure data handling, system interoperability, and continuous monitoring across distributed digital environments. These elements are essential for ensuring that intelligent cybersecurity systems remain scalable, reliable, and adaptable in increasingly interconnected technological ecosystems.

Overall, this research confirms that the convergence of artificial intelligence, big data analytics, and distributed security infrastructures forms a strategic foundation for enhancing cybersecurity resilience. Future research can further explore empirical validation of the proposed framework through simulation-based threat detection models, large-scale cybersecurity datasets, and real-world implementation scenarios in cloud computing, Internet of Things environments, and enterprise network security systems.

7. DECLARATIONS

7.1. About Authors

Syaifuddin (SS) https://orcid.org/0000-0002-6977-5256
Ahmad Gunawan (AG) https://orcid.org/0000-0003-2379-2576
Maulana Arif Komara (MA) https://orcid.org/0009-0005-8906-3132
Agung Lorenzo (AL) https://orcid.org/0009-0001-0362-5474

7.2. Author Contributions

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

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] A. Sarjito, "Technological pride and national resilience: How innovation shapes stability and security," *Jurnal Lemhannas RI*, vol. 12, no. 3, pp. 277–298, 2024.
[2] L. Z. Nasution, H. Siregar, R. Ismal, and T. Mariyanti, "Tawhidi string relationship (tsr) approach to entrepreneurial growth in waqf linked sukuk," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 701–712, 2025.
[3] P. Prabaswari, M. Alfikri, and I. Ahmad, "The implementation of policy for the establishment of a cyber incident response team to support information security in the government sector," *Matra Pembaruan*, vol. 6, no. 1, pp. 1–14, 2022.
[4] R. Anindita, V. H. Prastowo, and J. Parker, "Reinforcing the role of cyber village in improving indonesia msmes through an exploratory study," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 726–737, 2025.
[5] A. B. P. Kasmo, S. Mor, L. Nugroho, M. Rohadi, and A. Purnama, "Integrating corporate strategy with digital transformation, cybersecurity, and sustainability," *Jurnal Lemhannas RI*, vol. 13, no. 1, pp. 52–68, 2025.

[6] R. P. Wadipalapa, R. Katharina, P. P. Nainggolan, S. Aminah, T. Apriani, D. Ma'rifah, and A. L. Anisah, "An ambitious artificial intelligence policy in a decentralised governance system: evidence from indonesia," *Journal of Current Southeast Asian Affairs*, vol. 43, no. 1, pp. 65–93, 2024.

[7] P. A. Sunarya, R. A. Sunarjo, M. Abbas, O. A. Al-Kamari, and S. Maulana, "Ai-driven educational data analytics and intelligent tutoring in learning factory environments," *International Transactions on Education Technology (ITEE)*, vol. 4, no. 1, pp. 14–30, 2025.

[8] M. K. Gupta, A. K. Rai, M. Farooq *et al.*, "Network security and protection strategies for big data: Challenges and innovations," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 6. IEEE, 2023, pp. 705–709.

[9] 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.

[10] L. Diana, P. Dini, and D. Paolini, "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[11] N. Nuryani, A. B. Mutiara, I. M. Wiryana, D. Purnamasari, and S. N. W. Putra, "Artificial intelligence model for detecting tax evasion involving complex network schemes," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 339–356, 2024.

[12] M. Masunda and R. Ajayi, "Enhancing security in federated learning: designing distributed data science algorithms to reduce cyber threats," *Int J Adv Res Publ Rev*, vol. 2, no. 4, pp. 399–421, 2025.

[13] H. Herman, W. Achmad, N. Aulia, S. Rusdian, and T. Green, "Utilizing ipfs for decentralized data storage a security and censorship resistance solution," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 124–135, 2026.

[14] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks." *Artif. Intell. Rev.*, vol. 58, no. 4, p. 100, 2025.

[15] A. G. Prawiyogi, S. Purnama, and L. Meria, "Smart cities using machine learning and intelligent applications," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 102–116, 2022.

[16] X. Zhao, "Network security situational awareness and early warning architecture based on big data," *International Journal of System Assurance Engineering and Management*, pp. 1–17, 2024.

[17] A. Hlacs and H. Wells, "Using digital technology to strengthen oversight of public procurement in portugal: The use of data analytics and machine learning by the tribunal de contas," OECD Publishing, Paris, Tech. Rep. 83, Jun. 2025. [Online]. Available: https://doi.org/10.1787/43add03b-en

[18] T. S. Goh, S. Martinez, S. L. Sitorus, and T. L. Anita, "Adaptive strategic approaches and their impact on economic growth in dynamic markets," *Startupreneur Business Digital (SABDA Journal)*, vol. 4, no. 2, pp. 174–183, 2025.

[19] M. H. Kabir, M. Razib, Y. Arafat, R. A. M. Rashed, and Z. Jesan, "Strengthening us critical infrastructure resilience through nist-aligned cybersecurity governance and ai-driven threat detection," *Journal of Computer Science and Technology Studies*, vol. 7, no. 6, pp. 1120–1134, 2025.

[20] I. Sembiring, D. Manongga, U. Rahardja, and Q. Aini, "Understanding data-driven analytic decision making on air quality monitoring an empirical study," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 418–431, 2024.

[21] P. Nair and R. Yadavalli, "Hybrid ai-driven resilient architecture (hadra) for adaptive and autonomous cybersecurity: Analytical insights on emerging trends and challenges," in *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)*. IEEE, 2025, pp. 1–7.

[22] T. K. Chowdhury, "Ai-powered deep learning models for real-time cybersecurity risk assessment in enterprise it systems," *ASRC Procedia: Global Perspectives in Science and Scholarship*, vol. 1, no. 01, pp. 675–704, 2025.

[23] P. S. Sarker, S. K. Sadanandan, and A. K. Srivastava, "Resiliency metrics for monitoring and analysis of cyber-power distribution system with iots," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7469–7479, 2022.

[24] V. Tzavara and S. Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review," *International Journal of Information Security*, vol. 23, no. 3, pp. 1695–1719, 2024.

[25] A. Vaseashta, "Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and whole-of-government approach," in *Building cyber resilience against hybrid threats*. SAGE Publications 1 Oliver's Yard, 55 City Road, London, EC1Y 1SP, 2022, pp. 42–59.

[26] G. T. Sulistyantoro, A. Khaq, M. Z. K. Khan, A. Amin, and A.-A.-M. Hussain, "Shaping artificial intelligence governance and risk management in the public sector: Regulatory insights," *Lex Publica*, vol. 11, no. 1, pp. 161–181, 2024.

[27] M. S. Uddin, M. S. Sikder, M. M. Anwar, and F. Hossain, "Ai-driven cybersecurity and big data-enabled mis frameworks: Strengthening supply chain integrity, energy resilience, and critical infrastructure protection," *Journal of Computer Science and Technology Studies*, vol. 7, no. 9, pp. 223–232, 2025.

[28] A. Pratiwi, M. E. Rahmawyanet, P. A. W. Putra, D. I. Sensuse *et al.*, "Systematic literature review on artificial intelligence in indonesia's public sector: Reimagining digital government," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 11, no. 2, pp. 304–316, 2025.

[29] S. L. Sitorus, R. T. H. Safariningsih, A. H. A. N. Karsa, M. A. Komara, and R. Evans, "Optimizing smart contracts and blockchain for sustainable digital fashionpreneurship," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 37–48, 2025.

[30] I. E. Kezron, "Enhancing cybersecurity capacity in small and medium enterprises: A framework for workforce development," *Iconic Research And Engineering Journals*, vol. 7, no. 10, pp. 421–428, 2024.

[31] I. O. Evans-Uzosike, C. G. Okatta, B. Otokiti, O. Ejike, and O. T. Kufile, "Closing the cybersecurity talent gap: A strategic workforce readiness framework," *World Journal of Innovation and Modern Technology*, vol. 9, no. 6, pp. 230–241, 2025.

[32] I. R. Maulana, U. Rahardja, N. Azizah, M. Rakhmansyah, and M. A. Komara, "Leveraging ipfs to build secure and decentralized websites in the web 3.0 era," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 7, no. 1, pp. 1–12, 2025.

[33] A. N. Lone, S. Mustajab, and M. Alam, "A comprehensive study on cybersecurity challenges and opportunities in the iot world," *Security and Privacy*, vol. 6, no. 6, p. e318, 2023.

[34] R. Indrawan, A. Ratih, H. Agustian, and R. Evans, "Governance models for blockchain integrated iot ecosystems," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 219–229, 2026.

[35] J. Yu, A. V. Shvetsov, and S. H. Alsamhi, "Leveraging machine learning for cybersecurity resilience in industry 4.0: Challenges and future directions," *IEEE access*, vol. 12, pp. 159 579–159 596, 2024.

[36] P. Rathod, N. Polemi, M. Lehto, K. Kioskli, J. Wessels, and R. Lugo, "Leveraging the european cybersecurity skills framework (ecsf) in eu innovation projects: Workforce development through skilling, upskilling, and reskilling," in *2024 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2024, pp. 1–9.

[37] M. S. Islam, M. A. Rahman, M. A. Bin Ameedeen, H. Ajra, Z. B. Ismail, and J. M. Zain, "Blockchain-enabled cybersecurity provision for scalable heterogeneous network: A comprehensive survey." *Computer Modeling in Engineering & Sciences (CMES)*, vol. 138, no. 1, p. 43, 2024.

[38] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024.

[39] M. Siahaan, S. Kosasi, N. Sukendri, and A. Husain, "Enhancing smes business performance through strategic digital transformation," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 7, no. 1, pp. 85–96, 2025.

[40] M. M. I. Jabed, A. S. Khawer, S. Ferdous, D. H. Niton, A. B. Gupta, and M. S. Hossain, "Integrating business intelligence with ai-driven machine learning for next-generation intrusion detection systems," *International Journal of Research and Applied Innovations*, vol. 6, no. 6, pp. 9834–9849, 2023.

[41] B. Rawat, A. S. Bist, D. Apriani, N. I. Permadi, and E. A. Nabila, "Ai based drones for security concerns in smart cities," *APTISI Transactions On Management (ATM)*, vol. 7, no. 2, pp. 125–130, 2023.

[42] D. S. Mary, L. J. S. Dhas, A. Deepa, M. A. Chaurasia, and C. J. J. Sheela, "Network intrusion detection: An optimized deep learning approach using big data analytics," *Expert Systems with Applications*, vol. 251, p. 123919, 2024.

[43] A. Simanjuntak, A. Sutarman, S. A. Anjani, and A. Nuche, "Integrating artificial intelligence in e-learning for organizational well-being through orange technology mapping," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 7, no. 1, pp. 13–26, 2025.

[44] O. A. D. Wulandari, D. Apriani, and Y. Febriansyah, "Sustainable institutional entrepreneurial culture and innovation for economic growth," *APTISI Transactions on Management*, vol. 7, no. 3, pp. 221–230, 2023.

[45] W. Sun, A. Katsifodimos, and R. Hai, "Accelerating machine learning queries with linear algebra query processing," in *Proceedings of the 35th International Conference on Scientific and Statistical Database Management*, 2023, pp. 1–12.