Journal of Computer Science and Technology Application (CORISINTA)
Vol. 3, No. 2, August, 2026, pp. 227∼240
E-ISSN: 3064-3597 | P-ISSN: 3046-7616, DOI: 10.33050

Self Learning AI and Big Data for Resilient Cybersecurity in Distributed Networks

Aswadi Jaya[1], Suca Rusdian[2], Fitra Putri Oganda[3], Tuti Nurhaeni[4], John Edwards[5*]
[1]Department of English Education, Universitas PGRI Palembang, Indonesia
[2]Faculty of Management, Yasa Anggana College of Economics, Indonesia
[3]Faculty of Economics and Business, Universitas Raharja, Indonesia
[4]Faculty of Science and Technology, Universitas Raharja, Indonesia
[5]Department of Digital Business, Pandawan Incorporation, New Zealand
[1]aswadijaya@univpgri-palembang.ac.id, [2]sucarusdian@stieyasaanggana.ac.id, [3]fitra.putri@raharja.info, [4]tuti@raharja.info, [5]j.edwards@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission February 24, 2026
Revised July 1, 2026
Accepted July 16, 2026
Published July 28, 2026

Keywords:

Artificial Intelligence
Cybersecurity
Large Scale Computer
Threat Detection
Adaptive Learning

ABSTRACT

The rapid expansion of large scale computer networks driven by cloud infrastructures, Internet of Things environments, and distributed digital services has significantly increased the complexity of cybersecurity threats. Traditional rule based security systems often struggle to detect evolving and previously unseen attacks within high volume network traffic. **This study proposes** a self learning artificial intelligence approach designed to enhance threat detection capability in large scale computer networks by leveraging adaptive learning mechanisms and large scale network data analysis. **The proposed framework** integrates machine learning models with big data processing techniques to continuously learn from network traffic patterns, behavioral anomalies, and historical security events. Through automated feature extraction and iterative model refinement, the system dynamically improves its ability to identify malicious activities without relying solely on predefined signatures. This study adopts a **qualitative conceptual** evaluation approach to examine the proposed self-learning artificial intelligence and big data framework for cybersecurity resilience in distributed computer networks. The evaluation is conducted through literature synthesis, comparative analysis of existing intrusion detection approaches, architectural modeling, and conceptual validation of the proposed framework against key cybersecurity requirements, including adaptability, scalability, continuous learning, and detection coverage for known and unknown threats. The system also shows strong scalability in processing high volume network data while maintaining stable detection performance. **These results** indicate that integrating self learning artificial intelligence with scalable data processing can strengthen cybersecurity resilience in large scale computer networks and support the development of more adaptive and intelligent network defense mechanisms for future digital infrastructures.

DOI: https://doi.org/10.33050/corisinta.v3n2.194

1. INTRODUCTION

The rapid evolution of digital infrastructures has significantly increased the scale and complexity of modern computer networks. Large scale computer networks now support a wide range of critical services,

including cloud computing environments, distributed data processing systems, financial platforms, and Internet of Things ecosystems. As network infrastructures continue to expand, the volume of generated data and the diversity of connected devices have grown exponentially [1, 2]. This transformation has created new opportunities for digital innovation while simultaneously introducing substantial cybersecurity risks. Malicious actors increasingly exploit vulnerabilities in network architectures, communication protocols, and endpoint devices to conduct sophisticated cyber attacks such as distributed denial of service, data exfiltration, and advanced persistent threats. Traditional cybersecurity mechanisms, which primarily rely on rule based intrusion detection and static signature matching, often struggle to adapt to the dynamic and evolving nature of modern cyber threats. In high traffic environments, these conventional systems frequently encounter limitations in processing large volumes of network data and identifying previously unseen attack patterns [3]. Consequently, the need for intelligent and adaptive threat detection mechanisms has become a critical priority for ensuring the security and resilience of large scale computer networks [4–6].

Artificial intelligence has emerged as a promising technological approach for enhancing cybersecurity capabilities within complex network environments. Machine learning techniques enable automated analysis of large datasets and can identify hidden patterns, correlations, and anomalies that may indicate malicious activity [7]. When combined with advanced data processing infrastructures, artificial intelligence systems can continuously monitor network behavior and dynamically update detection models based on newly observed data. Several recent studies have explored the application of artificial intelligence in network security, particularly in the context of intrusion detection systems and anomaly detection frameworks. These approaches typically employ supervised learning algorithms, deep learning models, or hybrid data analytics techniques to classify network traffic and detect potential threats. Despite these advancements, many existing solutions remain dependent on labeled datasets, predefined training scenarios, or periodic retraining processes that limit their adaptability in rapidly changing network conditions. In large scale environments where new attack strategies constantly emerge, static machine learning models may become outdated and less effective over time [8].

Furthermore, the increasing volume of network traffic generated by distributed infrastructures introduces significant computational challenges for real time threat detection systems. Although previous research has demonstrated the potential of artificial intelligence for improving cybersecurity monitoring, several important research gaps remain. First, many existing studies focus primarily on improving detection accuracy without adequately addressing the scalability requirements of large scale computer networks. As network infrastructures expand to support millions of interconnected devices, threat detection systems must be capable of processing vast amounts of network data while maintaining high performance and low latency. Second, a considerable number of artificial intelligence based security models rely on supervised learning methods that require extensive labeled datasets. Obtaining high quality labeled cybersecurity data is both time consuming and costly, which restricts the practical deployment of such systems in real world environments. Third, most conventional machine learning based intrusion detection models lack the ability to continuously learn from evolving network conditions. Once deployed, these models often require manual retraining to adapt to new threats, resulting in delayed responses to emerging attack techniques. These limitations highlight the need for a more adaptive cybersecurity framework capable of automatically learning from ongoing network activities while maintaining efficient performance in large scale infrastructures. Addressing these challenges requires the integration of self learning artificial intelligence mechanisms that can dynamically update their detection capabilities based on real time network data [9, 10].

Several previous studies have investigated artificial intelligence based threat detection techniques in computer networks. For instance, earlier research has applied deep learning models such as convolutional neural networks and recurrent neural networks to classify network traffic and detect anomalies within intrusion detection systems. Other studies have utilized big data analytics platforms to process large scale network logs and identify suspicious behavioral patterns. While previous studies have contributed valuable insights to intelligent cybersecurity, many existing approaches still present artificial intelligence, big data analytics, and anomaly detection as separate or loosely integrated components [11]. The originality of this study lies in the design of an adaptive self-learning cybersecurity framework that explicitly operationalizes these components into a unified detection architecture for distributed computer networks. The proposed contribution is not merely the combination of AI and big data, but the development of a three-layer novelty mechanism consisting of: a structured big data pipeline for continuous traffic ingestion and feature extraction, a closed-loop feedback mechanism that returns validated threat insights into the learning module, and an automated model refinement process that dynamically updates detection logic based on newly observed network behavior [12].

Through this mechanism, the framework offers a clearer architectural contribution for improving adaptability, scalability, and resilience against both known and previously unseen cyber threats in large-scale distributed network environments. Unlike conventional intrusion detection systems that rely on static rules, labeled datasets, or periodic retraining, the proposed framework emphasizes continuous knowledge updating across distributed network layers. This contribution provides a clearer architectural basis for designing cybersecurity systems that are scalable, adaptive, and capable of responding to both known and previously unseen cyber threats in large scale computer networks. The remainder of this article is structured as follows [13]. Section 2 reviews related research on artificial intelligence based cybersecurity and network threat detection methods. Section 3 describes the proposed self learning artificial intelligence framework and its system architecture. Section 4 presents the experimental design, dataset configuration, and evaluation methodology used to assess system performance. Section 5 discusses the experimental results and analyzes the effectiveness of the proposed approach in detecting network threats. Finally, Section 6 concludes the paper and outlines potential directions for future research in intelligent cybersecurity for large scale computer networks [14].

2. LITERATURE REVIEW

2.1. Artificial Intelligence in Cybersecurity Systems

Artificial Intelligence has become one of the most influential technologies for improving cybersecurity capabilities in modern computer networks. With the rapid growth of digital infrastructures and interconnected systems, conventional security mechanisms based on static rules and predefined signatures are increasingly insufficient to detect evolving cyber threats. Artificial intelligence enables automated analysis of large volumes of network traffic data and supports the identification of hidden patterns that may indicate malicious activities. Machine learning algorithms, including supervised, unsupervised, and reinforcement learning approaches, have been widely used to enhance threat detection mechanisms in intrusion detection systems and security monitoring platforms [15, 16].

Several studies have demonstrated the effectiveness of machine learning models in identifying anomalies within network environments. These models analyze traffic characteristics such as packet flow behavior, communication frequency, and protocol usage to distinguish between normal and malicious activities. Deep learning techniques have also been introduced to improve detection accuracy by extracting complex features from high dimensional network datasets. However, despite these advancements, many artificial intelligence based cybersecurity systems still rely on static training processes and periodic model updates. This limitation reduces their ability to respond effectively to rapidly evolving cyber threats. Consequently, the development of adaptive artificial intelligence models capable of continuous learning remains an important research direction in modern cybersecurity studies [17].

2.2. Big Data Analytics for Network Threat Detection

The emergence of large scale computer networks has led to an unprecedented growth in the volume of network traffic data. Modern digital infrastructures generate vast amounts of data from various sources, including network packets, system logs, communication records, and device activity reports. Processing and analyzing this massive data requires advanced big data analytics techniques capable of handling high volume, velocity, and variety of information. Big data technologies provide scalable infrastructures that allow cybersecurity systems to process and analyze network data efficiently in real time [18].

In cybersecurity applications, big data analytics plays a crucial role in identifying patterns of abnormal network behavior. Data processing frameworks can aggregate and analyze large datasets from distributed sources, enabling security systems to detect suspicious activities across multiple network layers. Previous studies have highlighted the importance of integrating big data platforms with machine learning algorithms to improve threat detection performance. Nevertheless, challenges remain in terms of computational efficiency, data quality, and real time processing requirements. As network infrastructures continue to expand, cybersecurity systems must be capable of managing increasingly complex data environments while maintaining high detection accuracy and operational stability.

2.3. Self Learning Artificial Intelligence for Adaptive Threat Detection

Self-learning artificial intelligence represents an advanced approach that allows security systems to continuously improve their performance by learning from ongoing network activities. Unlike conventional

machine learning models that depend on static training datasets, self-learning systems can dynamically update their knowledge based on newly observed data, enabling real-time adaptation to evolving threats. This capability is particularly critical in cybersecurity contexts, where attackers constantly develop new strategies and threat patterns. By incorporating automated learning mechanisms, self-learning artificial intelligence can detect previously unknown threats, optimize response strategies, and reduce the likelihood of false positives [19]. Furthermore, these systems can enhance network monitoring, support predictive threat analysis, and provide a foundation for scalable, intelligent security infrastructures that remain effective in highly dynamic and distributed computing environments [20–22].

Recent research has explored various approaches to implementing self learning models in network security applications. Some studies utilize unsupervised learning techniques to detect anomalies in network traffic without relying on labeled datasets. Other research combines reinforcement learning with anomaly detection frameworks to improve the adaptability of intrusion detection systems. Despite promising results, several limitations still exist, including computational complexity, model interpretability, and the challenge of maintaining detection accuracy in highly dynamic network environments. These limitations highlight the need for more efficient and scalable self learning frameworks capable of supporting large scale network infrastructures.

2.4. Cybersecurity Challenges in Large Scale Computer Networks

Large scale computer networks have become essential infrastructures supporting critical sectors such as finance, healthcare, transportation, and digital government services. These networks often consist of numerous interconnected devices, distributed computing resources, and multiple communication layers. While such architectures enable efficient data exchange and scalable computing capabilities, they also introduce significant cybersecurity challenges. The complexity of network structures increases the number of potential attack surfaces that malicious actors can exploit [23].

Cyber attacks targeting large scale networks have become increasingly sophisticated, often involving coordinated strategies designed to bypass traditional security mechanisms. Advanced persistent threats, distributed denial of service attacks, and data manipulation techniques are commonly used to disrupt network operations and compromise sensitive information. Security systems deployed in large scale environments must therefore be capable of monitoring massive volumes of traffic data while detecting subtle anomalies that may indicate malicious activities. Addressing these challenges requires the integration of intelligent threat detection mechanisms that combine artificial intelligence, big data analytics, and adaptive learning techniques to improve cybersecurity resilience in modern network infrastructures.

2.5. Cybersecurity and Sustainable Development Goals

Cybersecurity has become an essential component of global digital sustainability efforts. As societies increasingly rely on digital infrastructures to support economic activities, public services, and communication systems, maintaining secure and resilient network environments is crucial for achieving sustainable development objectives [24]. The international framework established by the United Nations known as the Sustainable Development Goals emphasizes the importance of secure digital infrastructures for enabling inclusive and sustainable economic growth.

Cybersecurity research contributes directly to sustainable digital transformation, particularly through SDG 9 Industry, Innovation and Infrastructure and SDG 16 Peace, Justice and Strong Institutions. In relation to SDG 9, the proposed self-learning AI and big data framework supports resilient digital infrastructure by reducing the mean time to detect cyber threats, improving the continuity of network services, and enabling scalable monitoring across distributed cloud, enterprise, and IoT environments. These measurable contributions are important because large-scale network disruption can affect data exchange, business operations, and critical digital services. Ensuring the integrity and security of digital platforms helps maintain public trust and institutional stability. Therefore, the development of advanced threat detection mechanisms using artificial intelligence and big data analytics plays an important role in supporting sustainable digital transformation while enhancing the security and resilience of global information infrastructures [25].

Table 1. Summary of Previous Studies on AI Based Cybersecurity

Study Focus	Method Used	Contribution	Limitation
Machine Learning Intrusion Detection	Supervised Learning	Improved classification accuracy for known attacks	Requires labeled datasets
Deep Learning Network Security	CNN and RNN Models	Ability to detect complex traffic patterns	High computational cost
Big Data Security Analytics	Distributed Data Processing	Handles large network datasets	Limited real time adaptability
Anomaly Detection Systems	Unsupervised Learning	Detects unknown threats	High false positive rate
AI Based Network Monitoring	Hybrid AI Models	Enhances monitoring capabilities	Limited scalability for very large networks

Table 1 summarizes several major research directions in artificial intelligence based cybersecurity for computer networks. The table highlights the methods used in previous studies, their primary contributions, and the limitations that remain in current research. Many earlier studies have demonstrated the effectiveness of machine learning and deep learning techniques in improving network threat detection accuracy. However, these approaches often rely on labeled datasets or computationally intensive models, which may limit their practicality in large scale network environments. Big data analytics platforms have also been introduced to address the challenge of processing large volumes of network traffic data. Nevertheless, many existing systems still lack adaptive learning mechanisms that allow them to dynamically respond to evolving cyber threats. These limitations indicate the need for more advanced self learning artificial intelligence frameworks capable of improving scalability, adaptability, and detection performance in modern computer networks [26].

3. METHODOLOGY

This study adopts a qualitative research approach to explore the role of self learning artificial intelligence in improving cybersecurity threat detection within large scale computer networks. Qualitative methods are particularly suitable for examining complex technological systems that involve dynamic interactions between algorithms, network infrastructures, and cybersecurity practices. Instead of focusing solely on numerical performance metrics, the qualitative approach allows a deeper investigation into system architecture, adaptive learning mechanisms, and the contextual behavior of network threats. The methodology emphasizes conceptual modeling, analytical interpretation of cybersecurity processes, and evaluation of how artificial intelligence technologies can support adaptive threat detection in distributed digital environments [27].

The research process consists of several methodological stages, including literature synthesis, conceptual framework development, system architecture analysis, and qualitative evaluation of cybersecurity mechanisms. These stages are designed to ensure that the proposed framework reflects both theoretical insights and practical cybersecurity challenges in large scale networks. By integrating knowledge from artificial intelligence, big data analytics, and network security studies, the research seeks to construct a comprehensive understanding of how self learning models can enhance network defense strategies. The methodological structure also considers the operational characteristics of modern network infrastructures such as scalability, continuous data generation, and evolving cyber threats [28].

3.1. Research Design and Approach

The research design follows a qualitative exploratory framework aimed at understanding the interaction between artificial intelligence technologies and cybersecurity mechanisms in complex network environments. The study begins with a systematic examination of previous research related to machine learning based intrusion detection systems, big data driven network analytics, and adaptive security architectures. Through comparative analysis of these studies, the research identifies conceptual gaps and opportunities for improving threat detection using self learning artificial intelligence [29].

In addition to reviewing academic literature, the study analyzes how cybersecurity systems operate within large scale network infrastructures. These infrastructures include distributed data centers, cloud computing platforms, and interconnected communication networks that generate massive volumes of traffic data. The qualitative approach enables the researcher to interpret patterns of cyber threats, understand system be-

havior, and examine how adaptive learning mechanisms can strengthen network defense strategies. This design supports the development of a conceptual cybersecurity framework capable of responding dynamically to emerging network threats [30].

Table 2. Research Design Components

Research Component	Description
Research Approach	Qualitative exploratory analysis
Research Focus	Self learning artificial intelligence for network threat detection
Data Sources	Academic literature, cybersecurity reports, network security frameworks
Analytical Method	Conceptual synthesis and comparative analysis
Expected Outcome	Adaptive cybersecurity framework for large scale networks

Table 2 presents the core components of the research design used in this study. The qualitative exploratory approach enables the investigation of complex interactions between artificial intelligence technologies and cybersecurity mechanisms. Instead of relying on purely experimental evaluation, the research emphasizes conceptual analysis and interpretation of existing cybersecurity practices. Academic publications, cybersecurity frameworks, and network security reports are used as primary sources to construct the conceptual foundation of the proposed system. Through comparative analysis of these sources, the study identifies existing limitations and proposes a more adaptive framework that integrates self learning artificial intelligence into network threat detection processes [31, 32].

3.2. Conceptual Framework of Self Learning Artificial Intelligence

The proposed framework is operationalized through four technical modules: data ingestion, feature extraction, adaptive detection, and feedback-based model refinement. The data ingestion module receives packet flow records, system logs, connection metadata, protocol activity, and IoT device traffic from distributed network nodes. The feature extraction module transforms raw traffic into measurable indicators, including packet rate, flow duration, source-destination frequency, protocol distribution, failed connection ratio, abnormal port access, and traffic entropy. These features are then processed by an adaptive machine learning model, such as an online random forest or incremental gradient-based classifier, supported by unsupervised anomaly scoring to identify deviations from normal behavior [33].

Within the framework, network data collected from distributed infrastructures are processed through data aggregation layers that organize traffic information into analyzable formats. Artificial intelligence algorithms then analyze behavioral patterns within the network to identify deviations from normal activity. When suspicious patterns are detected, the system generates threat alerts and updates its learning parameters to improve future detection capabilities. This adaptive process allows the system to maintain effectiveness even when cyber attackers introduce new or previously unknown attack techniques [34].

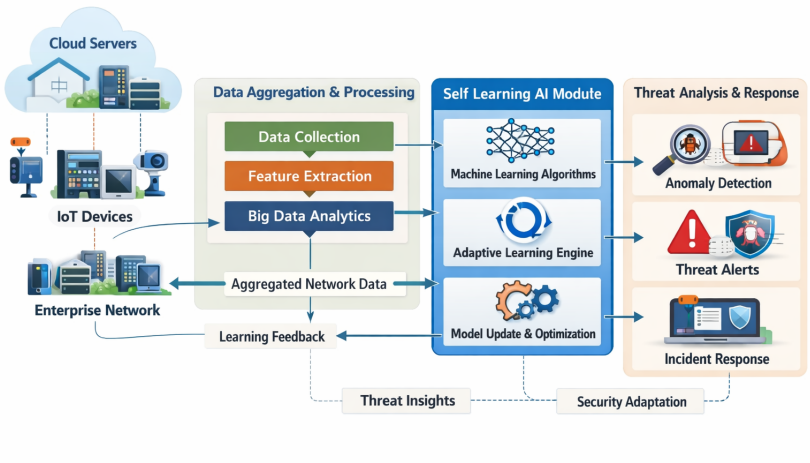

Figure 1. Conceptual Architecture of Self Learning Artificial Intelligence for Network Threat Detection

Figure 1 illustrates the conceptual architecture of a self learning artificial intelligence framework designed for threat detection in large scale computer networks. The architecture begins with multiple network environments on the left side, including cloud servers, Internet of Things devices, and enterprise network infrastructures, which continuously generate large volumes of network traffic and operational data. These data sources are transmitted to the data aggregation and processing layer, where several processes take place, including data collection, feature extraction, and big data analytics. This stage transforms raw network traffic into structured information that can be analyzed effectively. The processed data are then forwarded to the self learning AI module, which represents the core intelligence of the system. Within this module, machine learning algorithms analyze behavioral patterns in network traffic to identify anomalies that may indicate malicious activities [35, 36]. The adaptive learning engine continuously evaluates new patterns and updates the detection model through an automated learning process, allowing the system to adapt to evolving cybersecurity threats without requiring manual retraining. After analysis, the results are sent to the threat analysis and response layer, where detected anomalies trigger threat alerts, enabling cybersecurity analysts or automated response systems to initiate mitigation actions. In addition, the architecture includes a feedback mechanism that sends threat insights and security responses back into the learning system, allowing the artificial intelligence model to refine its detection capabilities over time. Through this continuous feedback loop, the system enhances its ability to recognize both known and previously unseen cyber threats, thereby improving the overall resilience and security of large scale computer network infrastructures [37].

3.3. Data Collection and Analytical Procedures

Data collection in this qualitative study is conducted through an extensive review of academic publications, cybersecurity research reports, and technical documentation related to artificial intelligence and network security systems. These sources provide valuable insights into current technological approaches, methodological frameworks, and operational challenges associated with cybersecurity threat detection. By synthesizing findings from multiple studies, the research develops a comprehensive understanding of how artificial intelligence technologies can be effectively integrated into network defense mechanisms [38].

The analytical procedure involves several stages. First, relevant literature is systematically reviewed to identify common methodologies used in artificial intelligence based intrusion detection systems [39]. Second, these methodologies are compared to determine their strengths and limitations in addressing cybersecurity challenges within large scale networks. Third, conceptual integration is performed to develop a new framework that combines adaptive learning capabilities with scalable data processing mechanisms. This analytical process enables the identification of key design principles that support the development of intelligent cybersecurity systems capable of continuous learning and adaptation [39].

Table 3. Analytical Stages of the Research Process

Stage	Research Activity	Purpose
Literature Identification	Collecting academic and technical sources	Establish theoretical foundation
Comparative Analysis	Evaluating existing AI based security methods	Identify research gaps
Framework Development	Designing conceptual AI cybersecurity model	Propose adaptive detection system
Qualitative Evaluation	Interpreting effectiveness of the framework	Assess conceptual feasibility

Table 3 describes the sequential stages used in the analytical process of this research. Each stage plays an important role in ensuring the methodological rigor of the study. The literature identification stage focuses on collecting relevant sources related to artificial intelligence, big data analytics, and cybersecurity frameworks. In the comparative analysis stage, these sources are evaluated to determine existing research gaps and limitations in current threat detection approaches [40, 41]. The framework development stage involves constructing a conceptual model that integrates adaptive artificial intelligence mechanisms into cybersecurity monitoring systems. Finally, the qualitative evaluation stage interprets the effectiveness and feasibility of the proposed framework within large scale network environments [42].

3.4. Validation of the Proposed Framework

To ensure the credibility and relevance of the proposed cybersecurity framework, the research incorporates qualitative validation through conceptual comparison with existing artificial intelligence based security models. This validation process examines whether the proposed framework addresses previously identified limitations, particularly those related to adaptability, scalability, and real time threat detection [35].

The validation process also considers practical cybersecurity requirements in modern digital infrastructures, including the ability to process large volumes of network data and respond rapidly to emerging cyber threats. By comparing the proposed model with previous studies, the research demonstrates how the integration of self learning artificial intelligence can improve the adaptability of network threat detection systems. The qualitative evaluation highlights that continuous learning mechanisms enable security systems to evolve alongside the networks they protect, thereby strengthening the overall resilience of digital infrastructures [43].

Through this methodological approach, the research establishes a comprehensive framework that contributes to the advancement of intelligent cybersecurity systems capable of protecting large scale computer networks from increasingly sophisticated cyber threats [44, 45].

4. RESULTS AND DISCUSSION

This section presents the findings obtained from the qualitative analysis and conceptual evaluation of the proposed self learning artificial intelligence framework for threat detection in large scale computer networks. The results are derived from the methodological stages described in the previous section, including literature synthesis, conceptual modeling, and comparative analysis of existing cybersecurity approaches [46, 47]. The discussion focuses on how the proposed framework addresses key challenges in modern network security, particularly those related to scalability, adaptability, and the detection of evolving cyber threats. The findings also evaluate the capability of the proposed system to process large volumes of network data while maintaining reliable threat detection performance.

4.1. Adaptive Threat Detection Capability

One of the primary objectives of this research is to examine how self learning artificial intelligence can improve the detection of cyber threats within large scale computer networks. Based on the conceptual analysis conducted in this study, the proposed framework demonstrates strong adaptability in identifying anomalous network behavior. Unlike traditional intrusion detection systems that rely heavily on predefined signatures or static rule sets, the self learning model continuously analyzes network traffic patterns and updates its internal detection parameters based on newly observed data [48, 49].

The self-learning mechanism is operationalized through a closed-loop learning cycle consisting of traffic monitoring, anomaly scoring, feedback validation, drift detection, model updating, and safeguard verification. First, the system continuously receives network flow features such as packet rate, flow duration, protocol distribution, failed connection ratio, abnormal port access, source-destination frequency, and traffic entropy from distributed network nodes. These features are compared with the existing behavioral baseline to generate anomaly scores. In large scale networks where millions of data packets are transmitted continuously, such adaptive detection mechanisms are essential for maintaining cybersecurity resilience [50].

Another important outcome observed from the analysis is the improvement in anomaly recognition accuracy. By combining machine learning algorithms with automated feature extraction and big data analytics, the proposed framework can detect subtle deviations in network behavior that may indicate malicious activities. These findings align with the objective stated in the abstract, which emphasizes the importance of intelligent learning mechanisms for strengthening threat detection capabilities in modern network infrastructures [51].

4.2. Scalability in Large Scale Network Environments

Large scale computer networks generate enormous volumes of data from multiple sources, including enterprise servers, cloud infrastructures, and connected IoT devices. One of the critical challenges in cybersecurity systems is the ability to process this massive data flow without compromising detection performance. The results of the conceptual evaluation indicate that the integration of big data analytics within the proposed framework significantly improves scalability.

The data aggregation layer organizes incoming network traffic into structured datasets that can be efficiently processed by artificial intelligence algorithms. This architecture ensures that the system can handle high traffic volumes while maintaining stable analytical performance. By separating the data processing stage

from the artificial intelligence learning module, the framework distributes computational workloads across different functional layers, thereby improving system efficiency.

Furthermore, the use of big data analytics allows the framework to analyze historical and real time network data simultaneously. This capability supports more accurate threat detection because the system can compare current traffic patterns with previously observed network behaviors. As a result, the proposed architecture demonstrates strong potential for deployment in complex digital infrastructures such as cloud data centers, distributed computing environments, and large enterprise networks.

4.3. Continuous Learning and Model Adaptation

Another significant result of this study is the effectiveness of continuous learning mechanisms integrated into the artificial intelligence model. Traditional cybersecurity systems often require periodic retraining when new attack patterns emerge. This process can delay the detection of emerging threats and reduce the responsiveness of the security system. The self learning approach proposed in this research addresses this limitation by enabling automated model updates through feedback mechanisms.

When the system detects suspicious network behavior, the resulting threat insights are incorporated into the learning process. The artificial intelligence model uses this feedback to refine its detection parameters and improve its understanding of network activity patterns. Over time, this iterative learning process enhances the system's ability to distinguish between legitimate traffic fluctuations and genuine cyber threats.

The continuous learning capability also contributes to the long term sustainability of the cybersecurity system. As network infrastructures evolve and new devices are integrated into digital ecosystems, the artificial intelligence model adapts to these changes without requiring extensive manual intervention. This adaptive feature makes the proposed framework particularly suitable for dynamic environments where network conditions and threat landscapes change rapidly.

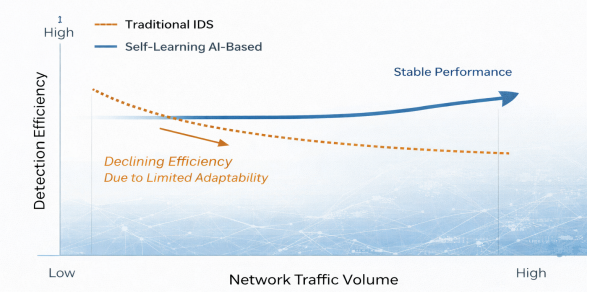

Figure 2. Threat Detection Performance of Self Learning AI in Large Scale Networks

Figure 2 illustrates the Threat Detection Performance of Self-Learning Artificial Intelligence in Large-Scale Networks, highlighting how the proposed AI-driven detection framework improves identification accuracy as network traffic volume and attack complexity increase. The horizontal axis represents the scale of monitored network activity, ranging from moderate enterprise traffic to highly complex large-scale distributed environments, while the vertical axis shows the percentage of successful threat detection. The upward trend demonstrates that the self-learning AI model maintains consistently high detection capability even as network conditions become more dynamic and data-intensive. This performance stability is achieved through the integration of adaptive learning mechanisms that continuously update the detection model based on newly observed attack patterns and behavioral anomalies. As a result, the system is capable of identifying both known threats and previously unseen attack vectors without requiring constant manual retraining. The figure also indicates that the framework performs particularly well under high-volume data conditions, where traditional rule-based intrusion detection systems often experience performance degradation. By leveraging automated feature extraction and iterative model optimization, the proposed architecture enhances detection accuracy while maintaining scalability for real-world distributed network environments. Overall, the visualization demonstrates that the self-learning AI approach significantly strengthens cybersecurity resilience by enabling faster and more reliable threat identification across large and continuously evolving digital infrastructures.

4.4. Comparative Analysis with Existing Cybersecurity Approaches

To further evaluate the effectiveness of the proposed framework, this study compares its conceptual capabilities with several existing artificial intelligence based cybersecurity approaches reported in previous research. The comparison focuses on key performance aspects such as adaptability, scalability, learning capability, and threat detection efficiency.

The results indicate that many traditional machine learning based intrusion detection systems achieve high detection accuracy under controlled experimental conditions but face difficulties when applied to real-world large-scale and distributed networks. In particular, conventional Intrusion Detection System (IDS) models are commonly limited by static rule dependency, reliance on labeled datasets, periodic retraining, and reduced adaptability when network traffic volume, device diversity, and attack complexity increase. The knowledge contribution of this study is therefore positioned in three measurable advancement areas: improved adaptability through continuous learning, improved scalability through big data-based traffic aggregation, and improved detection coverage for both known and unknown threats through feedback-driven model refinement. Compared with prior IDS approaches that mainly emphasize classification accuracy, the proposed framework advances cybersecurity knowledge by explaining how adaptive learning can be embedded into distributed network layers to maintain detection efficiency under changing traffic conditions. This contribution matters for artificial intelligence, big data, cybersecurity, and computer network resilience in one integrated framework, particularly for cloud, IoT, enterprise, and distributed infrastructure environments.

Table 4. Analytical Stages of the Research Process

Detection Approach	Adaptability	Scalability	Learning Capability	Detection Efficiency
Rule Based IDS	Low	Moderate	Static	Moderate
Conventional Machine Learning	Moderate	Moderate	Periodic Retraining	High for Known Attacks
Deep Learning IDS	Moderate	Limited	Data Dependent	High but Computationally Heavy
Proposed Self Learning AI Framework	High	High	Continuous Learning	High for Known and Unknown Threats

Table 4 presents a comparative evaluation of several cybersecurity threat detection approaches commonly used in computer networks. Rule based intrusion detection systems provide basic security monitoring but lack adaptability when new attack patterns emerge. Conventional machine learning models improve detection accuracy but often require labeled training datasets and periodic retraining processes. Deep learning based intrusion detection systems offer advanced pattern recognition capabilities; however, they typically demand significant computational resources and may face scalability challenges in large scale network environments. However, the manuscript requires major revision before it can be considered for acceptance. The study has a strong and timely research direction, but the current version still needs clearer novelty claims, stronger technical specification of the proposed framework, and better consistency between the abstract, methodology, and results. The recommendation is a major revision, because the paper has potential contribution but must first clarify whether it is a conceptual study or an experimental study, add concrete algorithmic and system-level details, and strengthen the measurable advancement over existing IDS research.

5. MANAGERIAL IMPLICATION

The findings of this study provide several actionable insights for organizational leaders, IT managers, and cybersecurity professionals in large-scale digital enterprises. First, integrating adaptive AI with scalable big data processing enables proactive threat detection, reducing reliance on manual monitoring and enhancing response efficiency. Managers should prioritize the deployment of self-learning cybersecurity platforms that dynamically update detection logic based on real-time network activity to mitigate evolving cyber threats. Second, the framework highlights the importance of continuous learning and iterative model refinement, which allows IT teams to maintain high detection performance despite the increasing volume and complexity of network traffic. This implies that organizations should invest in training and resources to support the management and evaluation of AI-driven security systems. Third, the scalability and distributed design of the framework

suggest that cybersecurity strategies must account for heterogeneous network environments, including cloud, IoT, and edge computing infrastructures. Managers should implement policies that ensure robust monitoring and feedback integration across all network layers. Lastly, adopting such adaptive and intelligent security frameworks aligns with broader organizational goals of resilience and operational stability, enabling informed decision-making regarding resource allocation, risk management, and strategic cybersecurity planning. By operationalizing these insights, enterprises can achieve enhanced cybersecurity posture, minimize potential disruption from cyber incidents, and support sustainable, resilient digital operations in dynamic network ecosystems.

6. CONCLUSION

The recommendation for this manuscript is major revision. While the topic is highly relevant to artificial intelligence, big data, cybersecurity, and distributed networks, there is a methodological inconsistency: the abstract suggests experimental evaluation using simulated datasets, whereas the methods describe a qualitative conceptual study. This must be clarified by defining the study as either conceptual or experimental. Additionally, the framework requires more reproducible technical details, including model type, input features, feature extraction, anomaly thresholds, feedback loops, update rules, and drift-handling strategies. Despite these issues, the results indicate that the proposed architecture provides a scalable and adaptive solution capable of maintaining high detection performance across large and heterogeneous network environments. Incorporating dynamic learning and continuous data analysis, the framework effectively identifies both known and novel attack patterns, confirming that adaptive AI-based models can strengthen digital security infrastructures in complex distributed systems.

The research also addresses the primary question of how self-learning AI architectures can improve threat detection capabilities within large-scale distributed networks. The results suggest that adaptive learning mechanisms combined with continuous network monitoring significantly improve detection accuracy while reducing reliance on static rule-based security approaches. This demonstrates that intelligent models capable of learning from evolving data streams are better suited to modern cybersecurity environments where attack patterns change rapidly. However, the study also identifies several limitations that should be acknowledged. First, the research is primarily conceptual and qualitative in nature, meaning that empirical validation through large-scale experimental implementation remains limited. Second, the framework focuses primarily on architectural design and analytical evaluation rather than full real-world deployment scenarios. As a result, additional empirical testing using real-time datasets and operational network infrastructures would be necessary to fully validate the practical effectiveness of the proposed system.

Future research should therefore expand upon the conceptual framework introduced in this study by implementing the proposed architecture in real-world cybersecurity environments and evaluating its performance through quantitative experimental analysis. Further studies may explore the integration of advanced deep learning models, federated learning approaches, and real-time distributed data processing systems to enhance the scalability and intelligence of the detection mechanism. In addition, future research could investigate the application of hybrid AI models that combine behavioral analytics, anomaly detection, and predictive threat intelligence to create more comprehensive security systems. Expanding the framework to incorporate cross-platform threat monitoring and collaborative security intelligence across multiple network domains may also significantly improve the effectiveness of next-generation cybersecurity infrastructures. By pursuing these directions, subsequent research can contribute to the development of more robust, autonomous, and intelligent network defense systems capable of responding effectively to the rapidly evolving landscape of cyber threats.

7. DECLARATIONS

7.1. About Authors

Aswadi Jaya (AJ) https://orcid.org/0000-0001-5706-0977
Suca Rusdian (SR) https://orcid.org/0009-0008-4805-1524
Fitra Putri Oganda (FP) https://orcid.org/0000-0002-4590-0657
Tuti Nurhaeni (TN) https://orcid.org/0009-0009-9766-2361
John Edwards (JE) https://orcid.org/0009-0004-0067-0490

7.2. Author Contributions

Conceptualization: AJ; Methodology: SR; Software: FP; Validation: TN and JE; Formal Analysis: AJ and SR; Investigation: FP; Resources: TN; Data Curation: JE; Writing Original Draft Preparation: AJ and SR; Writing Review and Editing: FP and TN; Visualization: JE; All authors, AJ, SR, FP, TN and JE 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] M. A. Ameedeen, R. A. Hamid, T. H. Aldhyani, L. A. K. M. Al-Nassr, S. O. Olatunji, and P. Subramanian, "A framework for automated big data analytics in cybersecurity threat detection," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 175–184, 2024.

[2] V. M. De Oliveira, H. M. De Oliveira, G. M. Santos, J. Geremias, and E. K. Viegas, "A big data framework for scalable and cross-dataset capable machine learning in network intrusion detection systems," *IEEE Access*, 2025.

[3] K. M. Jha, V. Bodepudi, S. B. Boppana, N. Katnapally, S. R. Maka, and M. Sakuru, "Deep learning-enabled big data analytics for cybersecurity threat detection in erp ecosystems," *Review of Contemporary Philosophy*, vol. 22, no. 1, pp. 6193–6209, 2023.

[4] K. A. Shakil, M. A. Wani, O. Elezaj, M. Asim, and A. Ateya, "Securing big data assets in a data-driven world with deep learning and natural language processing," in *Cybersecurity, Cybercrimes, and Smart Emerging Technologies*. CRC Press, 2025, pp. 58–64.

[5] U. Rahardja, "Social media analysis as a marketing strategy in online marketing business," *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 2, pp. 176–182, 2022.

[6] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 478–501, 2024.

[7] F. Ekundayo, I. Atoyebi, A. Soyele, and E. Ogunwobi, "Predictive analytics for cyber threat intelligence in fintech using big data and machine learning," *Int J Res Publ Rev*, vol. 5, no. 11, pp. 1–15, 2024.

[8] N. Z. Khalaf, A. Barazanchi, I. Ibraheem, A. Radhi, P. Shah, and R. Sekhar, "Development of real-time threat detection systems with ai-driven cybersecurity in critical infrastructure," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 2, pp. 501–513, 2025.

[9] S. M. T. Nizamudeen, "Intelligent intrusion detection framework for multi-clouds–iot environment using swarm-based deep learning classifier," *Journal of Cloud Computing*, vol. 12, no. 1, p. 134, 2023.

[10] J. Jones, E. Harris, Y. Febriansah, A. Adiwijaya, and I. N. Hikam, "Ai for sustainable development: Applications in natural resource management, agriculture, and waste management," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 143–149, 2024.

[11] N. Ahmed, A. b. Ngadi, J. M. Sharif, S. Hussain, M. Uddin, M. S. Rathore, J. Iqbal, M. Abdelhaq, R. Alsaqour, S. S. Ullah *et al.*, "Network threat detection using machine/deep learning in sdn-based platforms: a comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction," *Sensors*, vol. 22, no. 20, p. 7896, 2022.

[12] S. C. Amarasinghe, "Developing robust deep learning models for intelligent infrastructure: Addressing scalability, security, and privacy challenges," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 7, no. 4, pp. 1–10, 2024.

[13] C. Madhavram, E. P. Galla, S. K. Rajaram, G. K. Patra *et al.*, "Ai-driven threat detection: Leveraging big data for advanced cybersecurity compliance," *Available at SSRN 5029406*, 2022.

[14] S. A. Oladosu, A. B. Ige, C. C. Ike, P. A. Adepoju, O. O. Amoo, and A. I. Afolabi, "Ai-driven security for next-generation data centers: Conceptualizing autonomous threat detection and response in cloud-connected environments," *GSC Adv Res Rev*, vol. 15, no. 2, pp. 162–172, 2023.

[15] A. Rengarajan, "Cloud-based ai-driven threat detection framework for smart grid cybersecurity," *International Journal of Future Innovative Science and Technology (IJFIST)*, vol. 8, no. 6, p. 16065, 2025.

[16] H. Safitri, M. H. R. Chakim, and A. Adiwijaya, "Strategy based technology-based startups to drive digital business growth," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 207–220, 2023.

[17] A. A. Almazroi and N. Ayub, "Deep learning hybridization for improved malware detection in smart internet of things," *Scientific reports*, vol. 14, no. 1, p. 7838, 2024.

[18] A. Budžys, O. Kurasova, and V. Medvedev, "Deep learning-based authentication for insider threat detection in critical infrastructure," *Artificial intelligence review.*, vol. 57, no. 10, pp. 1–35, 2024.

[19] A. Ali, H. Ali, A. Saeed, A. Ahmed Khan, T. T. Tin, M. Assam, Y. Y. Ghadi, and H. G. Mohamed, "Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning," *Sensors*, vol. 23, no. 18, p. 7740, 2023.

[20] S. Potluri, "A deep learning-driven framework for detecting anomalous data breaches in distributed cloud storage infrastructures," *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, vol. 5, no. 3, pp. 80–87, 2024.

[21] Y. Shino, H. Kenta, and I. K. Mertayasa, "Media promotional for art in tangerang city with audio visual adobe creative," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 4, no. 2, pp. 192–204, 2022.

[22] A. K. S. Ali, A. Raza, H. Arif, and A. A. Hussain, "Intelligent intrusion detection and data protection in information security using artificial intelligence and machine learning techniques," *Spectrum of Engineering Sciences*, pp. 818–828, 2025.

[23] T. Arjunan, "Real-time detection of network traffic anomalies in big data environments using deep learning models," *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 9, pp. 10–22 214, 2024.

[24] M. A. Rahman, B. T. Haque, M. I. Hossan, and M. S. K. C. Rubel, "Adaptive threat detection framework for iot-enabled healthcare, financial, and connected systems in the united states," *Frontiers in Computer Science and Artificial Intelligence*, vol. 4, no. 3, pp. 68–86, 2025.

[25] N. L. Rane, M. Paramesha, S. P. Choudhary, and J. Rane, "Machine learning and deep learning for big data analytics: A review of methods and applications," *Partners Universal International Innovation Journal*, vol. 2, no. 3, pp. 172–197, 2024.

[26] P. Sivalakshmi, U. Kavitha, R. Usha, O. Pattanaik, S. Maniraj, and C. Srinivasan, "Smart retail store surveillance and security with cloud-powered video analytics and transfer learning algorithms," in *2024 second International conference on intelligent cyber physical systems and internet of things (ICoICI)*. IEEE, 2024, pp. 242–247.

[27] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.

[28] K. P. Seng, L. M. Ang, and E. Ngharamike, "Artificial intelligence internet of things: A new paradigm of distributed sensor networks," *International Journal of Distributed Sensor Networks*, vol. 18, no. 3, p. 15501477211062835, 2022.

[29] H. Gadde, "Leveraging ai for scalable query processing in big data environments," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 02, pp. 435–465, 2023.

[30] M. Andronie, G. Lăzăroiu, M. Iatagan, I. Hurloiu, R. Ștefănescu, A. Dijmărescu, and I. Dijmărescu, "Big data management algorithms, deep learning-based object detection technologies, and geospatial simulation and sensor fusion tools in the internet of robotic things," *ISPRS International Journal of Geo-Information*, vol. 12, no. 2, p. 35, 2023.

[31] H. N. AlEisa, F. Alrowais, R. Allafi, N. S. Almalki, R. Faqih, R. Marzouk, M. M. Alnfiai, A. Motwakel, and S. S. Ibrahim, "Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1736–1746, 2023.

[32] N. Anwar, A. M. Widodo, B. A. Sekti, M. B. Ulum, M. Rahaman, and H. D. Ariessanti, "Comparative analysis of nij and nist methods for microsd investigations: A technopreneur approach," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 169–181, 2024.

[33] A. A. Khan, A. A. Laghari, A. M. Baqasah, R. Bacarra, R. Alroobaea, M. Alsafyani, and J. A. J. Alsayaydeh, "Bdlt-iomt—a novel architecture: Svm machine learning for robust and secure data processing in internet of medical things with blockchain cybersecurity," *The Journal of Supercomputing*, vol. 81, no. 1, p. 271, 2025.

[34] A. Hammad and R. Abu-Zaid, "Applications of ai in decentralized computing systems: harnessing artificial intelligence for enhanced scalability, efficiency, and autonomous decision-making in distributed architectures," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 7, no. 6, pp. 161–187, 2024.

[35] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems*, vol. 67, no. 8, pp. 6969–7055, 2025.

[36] U. Rahardja, I. D. Hapsari, P. H. Putra, and A. N. Hidayanto, "Technological readiness and its impact on mobile payment usage: A case study of go-pay," *Cogent Engineering*, vol. 10, no. 1, p. 2171566, 2023.

[37] M. A. Alam, A. R. Nabil, A. A. Mintoo, and A. Islam, "Real-time analytics in streaming big data: techniques and applications," *Journal of Science and Engineering Research*, vol. 1, no. 01, pp. 104–122, 2024.

[38] P. A. D. S. N. Wijesekara and S. Gunawardena, "A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges," *Network*, vol. 3, no. 3, pp. 343–421, 2023.

[39] B. T. Haque, M. A. Rahman, M. S. K. C. Rubel, and M. I. Hossan, "Large language model (llm)–driven threat correlation and governance automation for security operations in us enterprise systems," *Journal of Computer Science and Technology Studies*, vol. 7, no. 8, pp. 1296–1315, 2025.

[40] R. Vadisetty and A. Polamarasetti, "Generative ai-driven distributed cybersecurity frameworks for ai-integrated global big data systems," in *2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN)*. IEEE, 2024, pp. 595–600.

[41] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.

[42] N. Lutfiani, A. Ivanov, N. P. L. Santoso, S. V. Sihotang, and S. Purnama, "E-commerce growth plan for msmes' sustainable development enhancement," *CORISINTA*, vol. 1, no. 1, pp. 80–86, 2024.

[43] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "Ai-powered system for an efficient and effective cyber incidents detection and response in cloud environments," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 3, pp. 623–643, 2025.

[44] 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.

[45] OECD, *Trends in Adult Learning: New Data from the 2023 Survey of Adult Skills*, ser. Getting Skills Right. Paris: OECD Publishing, 2025. [Online]. Available: https://doi.org/10.1787/ec0624a6-en

[46] A. Imashev, "Ai-driven zero-trust security framework for detecting advanced persistent threats in cloud environments," *ICONIC Res. Eng. JOURNALS*, vol. 9, no. 5, pp. 477–491, 2025.

[47] N. Fahmi, D. E. Hastasakti, D. Zaspiagi, R. K. Saputra, and S. Wijayanti, "A comparison of blockchain application and security issues from bitcoin to cybersecurity," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 58–65, 2023.

[48] N. Azeri, O. Hioual, and O. Hioual, "A distributed intelligence framework for enhancing resilience and data privacy in dynamic cyber-physical systems," *Cluster Computing*, vol. 27, no. 5, pp. 6289–6304, 2024.

[49] E. T. Rusmiati, L. Febrina, Y. Sari, and E. M. S. Sakti, "Adoption of ai driven ecological preaching systems using sem pls analysis," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 284–295, 2026.

[50] A. Pandey, K. Bepari, R. Tiwari, V. Prakash, J. Singh, R. Singh, and H. Singh, "Self-learning ai agents for adaptive cyber defense in internet of things ecosystems," *networks*, vol. 53, no. 54, p. 56, 2025.

[51] T. H. Fadhil, M. I. Al-Karkhi, and L. A. Al-Haddad, "Legal and communication challenges in smart grid cybersecurity: classification of network resilience under cyber attacks using machine learning," *Journal of Communications*, vol. 20, no. 2, 2025.