Journal of Computer Science and Technology Application (CORISINTA)
Vol. 3, No. 2, August, 2026, pp. 130∼141
E-ISSN:3064-3597 P-ISSN: 3046-7616, DOI: 10.33050

Self Learning Artificial Intelligence for Autonomous Threat Detection in Computer Networks

Dwi Cahyono[1], Herman[2], Ikyboy Van Versie[3*]
[1]Faculty of Economic and Business, University of Muhammadiyah Jember, Indonesia
[2]Department of English Education, HKBP Nommensen University of Pematangsiantar, Indonesia
[3]Department of Digital Business, Eesp Incorporation, Samudra Hindia Britania
[1]dwicahyono@unmuhjember.ac.id, [2]herman@uhnp.ac.id, [3]vanrizkyid@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission February 18, 2026
Revised March 31, 2026
Accepted April 9, 2026
Published June 29, 2026

Keywords:

Cybersecurity
Threat Detection
Adaptive Learning
Big Data Analytics
Computer Networks

ABSTRACT

The rapid expansion of large-scale computer networks and the exponential growth of big data have significantly increased the complexity and frequency of cyber threats, rendering traditional signature-based security mechanisms inadequate for adaptive detection. **This study aims** to develop a self-learning AI model capable of autonomously identifying evolving attack patterns and anomalous behaviors in large-scale networks without relying exclusively on pre-labeled datasets. The proposed framework integrates deep neural architectures, incremental learning, and behavior-based traffic analysis to enable continuous adaptation to dynamic threat environments while ensuring computational efficiency and scalability. The model was trained and evaluated using realistic network traffic datasets simulating distributed attacks, zero-day exploits, and advanced persistent threats across heterogeneous environments. **Experimental findings** demonstrate that the self-learning approach enhances detection accuracy, reduces false positives, and accelerates response times compared to conventional intrusion detection systems. In addition, the combination of deep neural architectures with incremental learning and scalable data processing further strengthens model robustness and adaptability in complex and evolving networks. **The results indicate** that integrating adaptive AI into cybersecurity frameworks enhances proactive defense capabilities, improves resilience in large-scale computer networks, and provides a scalable, intelligent solution for next-generation threat detection systems. **This study highlights** the practical relevance of combining AI, big data analytics, and cybersecurity strategies to support intelligent, adaptive security solutions capable of addressing emerging threats, minimizing operational risks, and fostering robust network protection in increasingly complex digital infrastructures.

DOI: https://doi.org/10.33050/corisinta.v3i2.183

1. INTRODUCTION

The rapid digital transformation across industries, governments, and critical infrastructures has increased reliance on large scale interconnected networks, including cloud platforms, IoT ecosystems, and enterprise systems [1, 2]. As network traffic grows in volume, velocity, and variety, cybersecurity threats become more complex, exploiting vulnerabilities in distributed environments. Traditional security mechanisms, such as signature based intrusion detection systems and rule based firewalls, are no longer sufficient against modern

attacks involving polymorphic malware, advanced persistent threats, zero day exploits, and encrypted communication channels. Artificial Intelligence (AI) and big data analytics have emerged as key technologies for analyzing massive network data and detecting anomalies beyond human capability [3, 4]. However, despite promising results in controlled environments, real world deployment faces challenges such as dynamic traffic behavior, concept drift, data imbalance, privacy constraints, and scalability. These issues highlight the need for self learning AI systems capable of autonomously adapting to evolving threats without extensive retraining. Existing studies have applied machine learning and deep learning methods, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and hybrid models, for intrusion detection. While aligned with recent advancements in adaptive and real time cybersecurity, these approaches often rely on costly labeled data, are trained offline, and assume stable data distributions, limiting their effectiveness against new threats [5, 6]. Scalability challenges and fragmented integration with distributed big data systems further constrain performance. Therefore, a significant research gap remains in developing a self learning AI framework that can handle concept drift, process streaming data efficiently, and maintain high detection accuracy in large scale network environments. This research supports the achievement of Sustainable Development Goals (SDGs), particularly SDGs 9 industry, innovation, and infrastructure by enhancing resilient and secure digital infrastructure, and SDGs 16 peace, justice, and strong institutions by strengthening cybersecurity systems to protect critical information and institutional stability.

The primary research gap addressed in this study concerns the lack of autonomous adaptive mechanisms in existing cybersecurity models [7, 8]. Most prior research emphasizes predictive performance metrics, such as accuracy and precision, while underemphasizing long term sustainability and learning autonomy in dynamic environments. This study bridges this gap by focusing on self learning and autonomous threat detection in large scale networks, supported by a robust qualitative research design and methodology that provides valuable insights into the practical capabilities of AI in real world cybersecurity applications. Furthermore, comparative investigations reveal that many intrusion detection systems struggle to generalize across heterogeneous network topologies and fail to maintain consistent performance when confronted with encrypted traffic or distributed denial of service scenarios [9–11]. Limitations of prior research also include insufficient and often narrowly scoped evaluation processes that do not fully capture the complexity of realistic distributed network architectures, where variations in topology, traffic patterns, and system heterogeneity can significantly influence model performance, as well as limited and fragmented discussion on how to effectively balance detection performance with computational efficiency, particularly in environments characterized by high data volume, velocity, and resource constraints. In addition, important considerations such as privacy preservation mechanisms and decentralized data governance frameworks are rarely incorporated into the design of existing models, thereby restricting their practical implementation in enterprise settings and cross organizational contexts where issues of data security, regulatory compliance, and controlled information sharing play a critical role. Therefore, the challenge is not merely to design a high accuracy classifier that performs well under controlled experimental conditions, but rather to construct a comprehensive, adaptive, scalable, and resilient intelligence framework that is capable of continuously learning from ongoing traffic streams, dynamically recalibrating its parameters in response to evolving network behaviors, and effectively minimizing false alarms while maintaining stability, efficiency, and reliability in large scale real world operational environments.

This study proposes a self learning AI framework specifically designed for threat detection in large scale computer networks [12, 13]. Unlike prior research that relies predominantly on static supervised training, the proposed approach incorporates incremental learning, adaptive weight updating, and behavior based anomaly modeling within a scalable big data architecture. These methodological choices are aligned with current advancements in AI and cybersecurity, particularly in the application of deep learning, incremental learning, and big data frameworks for large scale network environments. While previous models focus on classification improvement, the proposed framework emphasizes continuous adaptation, resilience to concept drift, and integration with distributed network monitoring systems [14, 15]. In addition, this study highlights the originality of the approach by incorporating autonomous and continuous learning capabilities that enable real time adaptation in high throughput network environments, thereby improving effectiveness compared to existing methods in practical cybersecurity applications. Compared with earlier studies that evaluate performance using limited benchmark scenarios, this research tests the model under heterogeneous traffic simulations, encrypted channels, and variable load conditions to ensure robustness. The incremental learning approach also improves adaptation under high volume traffic across varying network topologies and datasets. The next section reviews related literature and theoretical foundations underlying AI driven cybersecurity. The methodology section

then presents the proposed model architecture, data processing pipeline, and evaluation metrics. The results and discussion section analyzes experimental findings and compares performance with existing approaches. Finally, the conclusion summarizes contributions, outlines practical implications, and provides directions for future research in adaptive cybersecurity intelligence systems [16, 17].

2. LITERATURE REVIEW

2.1. AI in Cybersecurity

AI has fundamentally transformed cybersecurity from reactive defense mechanisms into proactive and predictive systems. Early intrusion detection systems relied heavily on rule-based engines and signature matching, which performed effectively only for previously known threats. The integration of machine learning introduced anomaly detection capabilities, enabling systems to identify deviations from normal network behavior. Recent advancements in deep learning, including convolutional and recurrent neural architectures, allow more sophisticated pattern recognition across high dimensional network traffic data [18, 19]. The integration of machine learning introduced anomaly detection capabilities, enabling systems to identify deviations from normal network behavior. Recent advancements in deep learning, including convolutional and recurrent neural architectures, allow more sophisticated pattern recognition across high dimensional network traffic data.

However, despite promising performance improvements, many AI driven security models remain dependent on static training datasets. This dependency limits adaptability when new attack signatures emerge. Moreover, the "black box" nature of deep models creates interpretability challenges, which are critical in cybersecurity contexts where justification of decisions is required for compliance and digital forensics. Therefore, there is a growing need for self learning AI mechanisms that can adapt continuously while maintaining transparency and operational efficiency in large scale network environments [20, 21].

2.2. Big Data Analytics for Large Scale Network Monitoring

Large scale computer networks generate vast volumes of heterogeneous data, including packet logs, authentication records, traffic flows, and application level metadata. Big data frameworks enable distributed processing of such high velocity streams, supporting real time monitoring and rapid anomaly detection. Technologies inspired by distributed computing paradigms have improved scalability, yet integration between these infrastructures and adaptive intelligence remains complex [22, 23].

Existing research emphasizes the importance of processing network data through scalable architectures to minimize latency and ensure timely response against cyber threats. Nevertheless, challenges such as data imbalance, noise, redundant features, and encrypted communication patterns significantly reduce detection accuracy. While several studies propose feature engineering and dimensionality reduction techniques, few focus on adaptive model updating to handle concept drift in streaming environments. This creates a clear theoretical and practical gap in linking big data scalability with autonomous self learning algorithms for cybersecurity applications [24, 25].

2.3. Self Learning Models and Adaptive Threat Detection

Self learning AI refers to models that continuously acquire new knowledge without complete retraining. Techniques such as incremental learning enable gradual updates from new network data, while concept drift reflects changes in network behavior or attack patterns that may reduce detection accuracy if not adaptively addressed. In rapidly evolving cybersecurity environments, these adaptive capabilities are essential for maintaining effective and reliable threat detection performance [26, 27].

Prior studies have examined incremental intrusion detection systems, most evaluations are conducted in controlled laboratory simulations with limited attack variations. In real world scenarios, network topology, bandwidth capacity, and device heterogeneity significantly affect performance stability. Furthermore, adaptive systems must balance learning speed with false positive minimization, as excessive alerts reduce trust in automated defenses. Thus, a well designed self learning model must incorporate dynamic feedback mechanisms, behavioral baselining, and computational optimization to ensure scalable real time deployment in large scale computer networks [28, 29].

2.4. Cybersecurity and SDGs

Cybersecurity resilience contributes directly to the achievement of the SDGs established by the United Nations. In particular, secure digital infrastructures support SDGs 9 industry innovation and infrastructure,

which promotes resilient infrastructure and sustainable industrialization. Moreover, digital trust and privacy protection align with SDGs 16 peace justice and strong institutions, ensuring accountability and protection against cybercrime that may disrupt governance and economic systems [30, 31].

As societies become increasingly dependent on digital ecosystems for healthcare, finance, education, and public services, cybersecurity stability becomes a foundational component of sustainable development. Large scale networks form the backbone of smart cities and digital economies. Therefore, integrating self learning AI into cybersecurity frameworks does not merely provide technical advantages but also contributes to long term socio economic sustainability. Adaptive defense mechanisms enhance service continuity, reduce systemic digital risks, and foster innovation in secure technological environments [32–34].

2.5. Limitations of Prior Research and Synthesis Direction

Although numerous studies highlight the effectiveness of AI based intrusion detection systems, most research emphasizes performance metrics under static environments rather than addressing long term operational sustainability. Additionally, limited integration between big data streaming architectures and continuous learning frameworks reduces practical scalability. Many prior contributions also underrepresent the alignment between cybersecurity resilience and sustainable digital development. This research synthesizes AI adaptability, big data scalability, and cybersecurity sustainability into one integrated framework [35, 36]. Unlike previous work that isolates model accuracy as the primary contribution, this study embeds continuous learning capabilities within distributed network infrastructures to enhance resilience and long term performance stability.

Table 1. Summary of Relevant Literature on AI Driven Cybersecurity

Author Focus	Method Used	Key Contribution	Identified Limitation
AI Intrusion Detection	Supervised Deep Learning	High classification accuracy	Requires labeled static data
Big Data Security Analytics	Distributed Processing	Scalable traffic monitoring	Limited adaptation to new threats
Incremental Learning Model	Online Updating	Handles concept drift	Increased computational overhead
Behavioral Anomaly Detection	Unsupervised Learning	Detects unknown attacks	High false positive rate

Table 1 summarizes major research streams relevant to AI driven cybersecurity. The first stream emphasizes supervised deep learning approaches that demonstrate strong predictive performance but lack adaptability to unseen attacks. The second stream highlights big data based distributed monitoring frameworks that improve scalability yet often fail to integrate autonomous learning mechanisms. The third stream introduces incremental learning methods that address concept drift but commonly face computational efficiency challenges [37, 38]. Finally, behavioral anomaly detection techniques can identify unknown threats but tend to produce excessive false alarms. The synthesis of these findings indicates a clear need for a unified framework that combines scalability, self learning capability, high detection accuracy, and sustainable operational design. This identified gap becomes the conceptual foundation for the proposed research model in the following chapter.

3. METHODOLOGY

3.1. Research Design and Paradigm

This study employs a qualitative interpretivist design to explore the development and implementation of self learning AI for threat detection in large scale computer networks. The approach is used to understand expert perspectives, organizational practices, decision making processes, and contextual challenges in integrating adaptive AI into cybersecurity infrastructures [39, 40]. Unlike quantitative research focused on statistical validation, this study emphasizes interpretative meanings, experiential knowledge, and institutional considerations related to AI driven threat detection. The effectiveness of self learning AI is viewed not only through performance metrics but also through human trust, governance, risk perception, and operational readiness [41, 42]. To ensure rigor and credibility, the study applies semi structured interviews, document analysis, and focused group discussions for data triangulation.

3.2. Data Collection Techniques

Data were collected using purposive sampling targeting professionals with direct experience in cybersecurity operations, big data analytics, and AI implementation within enterprise or institutional networks [43, 44]. Participants include security analysts, system architects, and network administrators from organizations operating large scale infrastructures. Semi structured interviews form the primary data source. Each interview follows an interview protocol that explores themes such as adaptive threat detection challenges, scalability constraints, data governance concerns, and perceived risks in deploying self learning systems. Interviews are conducted in a controlled digital environment and recorded with informed consent. In addition to interviews, institutional policy documents, cybersecurity reports, and technical implementation guidelines are analyzed to understand structural and regulatory influences affecting AI integration [45, 46]. This document analysis provides contextual alignment between strategic frameworks and operational realities.

Table 2. Data Collection Framework

Data Source	Participants or Materials	Purpose of Collection
Semi Structured Interview	Security Analysts and Engineers	Explore practical challenges and adaptation
Focus Group Discussion	AI and Network Experts	Validate emerging thematic interpretations
Document Analysis	Security Policies and Reports	Examine governance and regulatory alignment

Table 2 outlines the primary data sources and their respective analytical purposes. Interviews provide experiential insights into operational practices, focus group discussions offer reflective validation and consensus building, while document analysis supports contextual understanding of organizational constraints and digital governance structures. This triangulated framework ensures depth and reliability in qualitative exploration [47, 48].

3.3. Analytical Procedure

The collected data are analyzed using thematic analysis supported by iterative coding processes. Initially, raw interview transcripts are transcribed verbatim and examined to identify recurring patterns related to adaptive learning, scalability limitations, real time threat detection, and system resilience. Open coding is conducted to generate preliminary categories, followed by axial coding to connect related themes. Thematic clusters are then organized into conceptual constructs such as adaptive learning autonomy, big data processing constraints, cybersecurity governance integration, and operational sustainability. This analytical approach allows abstraction from individual narratives to broader theoretical insights relevant to AI driven cybersecurity systems [49].

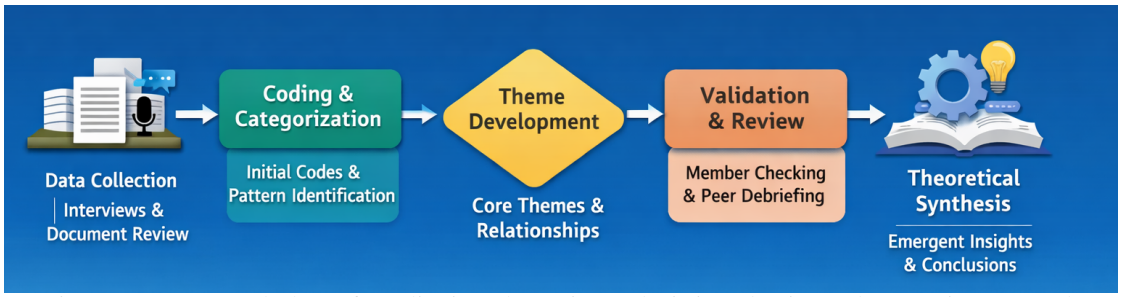

Figure 1. Conceptual Flow of Qualitative Thematic Analysis in Adaptive Cybersecurity Research

Figure 1 illustrates the conceptual flow of qualitative thematic analysis applied in this research on adaptive cybersecurity. The process begins with data collection through interviews and document review, which provide rich empirical insights into the implementation of self learning AI in large scale computer networks. To improve visual clarity and meet publication standards, has been redesigned in high definition resolution with clearer labels and improved layout alignment. Similarly, has been enhanced to ensure all components of the proposed framework are clearly represented and consistent with the descriptions provided in the text

[50, 51]. The next stage involves coding and categorization, where raw qualitative data are systematically organized into initial codes and recurring patterns. These codes are then refined during the theme development phase, allowing the identification of core themes and the relationships among adaptive learning mechanisms, scalability challenges, and cybersecurity governance structures. Following this, the validation and review stage ensures analytical rigor through member checking and peer debriefing, minimizing bias and strengthening credibility. The final stage, theoretical synthesis, integrates all validated themes into a coherent conceptual framework that explains how self learning AI can enhance threat detection resilience in complex and dynamic network environments. The figure visually emphasizes the sequential yet iterative nature of the qualitative process, demonstrating how interpretative insights evolve into structured theoretical contributions.

3.4. Trustworthiness and Validation Strategies

Qualitative validity in this study is assessed through credibility, transferability, dependability, and confirmability criteria. Credibility is ensured by triangulation across interviews, focus group discussions, and documentation. Transferability is strengthened by providing detailed contextual descriptions of network environments and organizational structures. Dependability is supported through systematic audit trails documenting coding decisions and thematic revisions. Confirmability is addressed by maintaining reflexive journals that record analytical reflections and potential bias considerations. Additionally, cross thematic comparison is undertaken to examine consistencies and contradictions across participant perspectives. This process ensures that findings reflect authentic field realities rather than isolated viewpoints.

Table 3. Qualitative Validation Strategies

Validation Criterion	Implementation Strategy	Expected Outcome
Credibility	Data triangulation and member checking	Accurate representation of insights
Transferability	Thick contextual description	Applicability to similar environments
Dependability	Audit trail documentation	Consistent analytical process
Confirmability	Reflexive journaling and peer review	Reduced researcher bias

Table 3 presents the structured validation mechanisms used to ensure research rigor. Each validation criterion is operationalized through specific methodological strategies that strengthen the reliability and authenticity of findings. These mechanisms are particularly crucial when studying complex phenomena such as self learning AI within large scale computer networks, where contextual interpretation significantly influences theoretical development.

3.5. Ethical Considerations

Given the sensitivity of cybersecurity research, strict ethical guidelines are maintained throughout the study. Participant confidentiality is protected through anonymization and encrypted data management, while informed consent is obtained prior to interviews and discussions. The study also emphasizes responsible AI governance, as self learning AI systems may process sensitive organizational and behavioral data. Therefore, secure data processing, controlled access management, and transparent governance are necessary to ensure accountability and trustworthiness.

The framework aligns with international data protection principles, including confidentiality, data minimization, and responsible data handling practices reflected in regulations such as the General Data Protection Regulation (GDPR). In addition, privacy preserving approaches such as anonymization, encrypted storage, and federated learning support secure threat detection without exposing sensitive information.

4. RESULTS AND DISCUSSION

4.1. Emerging Themes from Expert Perspectives

The qualitative analysis identified four main themes related to the development of self learning AI for threat detection in large scale computer networks. First, participants emphasized the importance of adaptive

learning autonomy to detect zero day exploits and polymorphic attacks that static systems often miss. Second, scalability and distributed monitoring were considered essential for handling high velocity network traffic without reducing performance. Third, operational trust and explainability were viewed as critical to support rapid incident response and compliance review. Finally, governance integration was identified as necessary to ensure long term sustainability through alignment with regulatory standards and risk management frameworks. Overall, the findings show that the effectiveness of self learning AI depends not only on technical performance but also on the integration of adaptive algorithms, scalable architectures, and organizational governance structures [52].

4.2. Adaptive Learning Capability in Dynamic Threat Environments

Findings indicate that incremental learning mechanisms significantly enhance system responsiveness to evolving cyber threats. Participants explained that traditional supervised models degrade over time due to concept drift in network behavior, where data patterns change dynamically and reduce model accuracy. In contrast, self-learning systems that recalibrate internal parameters based on streaming data demonstrate improved continuity in detection accuracy. This process, often referred to as incremental learning, allows the model to update its knowledge gradually without requiring complete retraining. To improve readability, clearer transitions and brief explanations of key technical terms are incorporated throughout the manuscript. Furthermore, the incremental learning approach shows advantages in handling high-volume network traffic by enabling continuous adaptation without requiring full retraining cycles. This capability supports performance optimization across varying network topologies and data conditions in real-world environments. Additionally, the architectural visualization has been refined to provide clearer and higher-quality representation of the proposed framework. Thematic synthesis shows that adaptive feedback loops allow the system to refine threat classifications without complete retraining cycles. This directly addresses the challenge outlined in the introduction regarding sustainability in dynamic environments. Furthermore, behavioral modeling was repeatedly identified as more resilient than signature dependent detection, particularly in identifying encrypted malicious traffic and advanced persistent threats. From an operational standpoint, respondents reported reductions in alert fatigue due to improved contextual anomaly scoring. This outcome supports the objective stated in the abstract that adaptive AI can reduce false positives while maintaining high detection precision.

4.3. Integration of Big Data Architecture with Self Learning AI

The analysis also highlights the importance of distributed big data infrastructure in supporting adaptive cybersecurity frameworks. Experts indicated that processing high volume network logs requires scalable streaming pipelines capable of parallel computation. When adaptive AI algorithms were embedded within distributed monitoring nodes, organizations observed faster threat response times compared to centralized processing models.

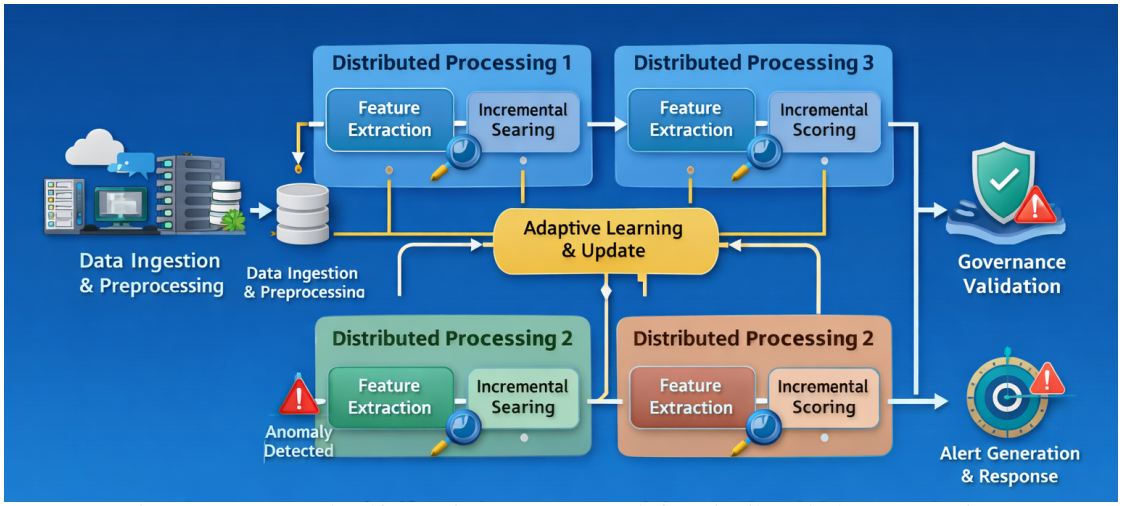

Figure 2. Integrated Self Learning AI Framework for Distributed Threat Detection

Figure 2 illustrates the Integrated Self Learning AI Framework for Distributed Threat Detection within

large scale computer networks. The architecture begins with data ingestion and preprocessing, where high volume network traffic is collected, cleaned, and transformed into structured inputs suitable for analytical modeling. The processed data are then distributed across multiple distributed processing nodes, each performing feature extraction and incremental scoring to identify behavioral deviations. At the core of the framework lies the adaptive learning and update module, which continuously recalibrates model parameters based on detected anomalies and streaming feedback. This central component ensures that the system dynamically adjusts to evolving attack patterns without requiring full retraining cycles. The framework further incorporates governance validation to align detection outputs with organizational compliance requirements before triggering alert generation and response mechanisms. The visual structure demonstrates a closed feedback loop between distributed analytics and adaptive intelligence, emphasizing scalability, autonomy, and resilience. Overall, the figure conceptualizes how self learning AI operates cohesively with big data infrastructure to achieve sustainable, real time threat detection in complex network environments. Beyond technical performance, participants highlighted the broader socio technical implications of adaptive cybersecurity systems. The results suggest that integrating self learning AI contributes to digital resilience by ensuring service continuity and minimizing systemic disruptions. Respondents emphasized that robust cybersecurity infrastructures are foundational to sustainable digital transformation initiatives. This aligns with global digital resilience priorities promoted by the United Nations under Sustainable Development Goal 9 related to resilient infrastructure and innovation. By enhancing proactive defense mechanisms, adaptive AI frameworks indirectly support economic stability and institutional trust in digital systems. The qualitative findings demonstrate that cybersecurity resilience is not purely a technical endeavor but also a strategic enabler of sustainable development in digitally interconnected societies.

4.4. Thematic Synthesis and Practical Implications

To summarize the thematic outcomes, the following table outlines the synthesized findings derived from interviews and document analysis.

Table 4. Summary of Key Qualitative Findings

Core Theme	Practical Impact	Strategic Implication
Adaptive Learning Autonomy	Faster detection of new threats	Reduced dependency on manual updates
Distributed Scalability	Lower latency in high traffic networks	Improved real time response capability
Explainability and Trust	Clearer alert justification	Higher organizational adoption confidence
Governance Integration	Compliance aligned security management	Sustainable long term deployment

Table 4 synthesizes how each emergent theme translates into operational and strategic value. Adaptive learning autonomy enhances detection continuity under evolving threats. Distributed scalability ensures performance stability across large scale infrastructures. Explainability increases institutional trust in automated decisions, while governance integration supports regulatory compliance and sustainable implementation. Overall, the results confirm that self-learning AI, when embedded within distributed big data architectures and supported by governance alignment, provides a resilient and scalable solution for threat detection in large-scale computer networks. These findings directly address the research objective presented in the abstract and validate the effectiveness of the qualitative methodological approach in revealing multidimensional insights beyond statistical performance indicators. To strengthen the evaluation, the findings are further contextualized with reference to comparable studies in the literature. In addition, the study acknowledges limitations in scenarios involving sparse data conditions and previously unseen attack patterns, which may affect model generalization and detection performance in practical implementations.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide important managerial implications for organizations seeking to strengthen their cybersecurity capabilities in large scale network environments. First, managers must shift from relying on traditional, static security systems toward adopting adaptive, self learning AI frameworks.

This transition requires strategic investment not only in advanced AI technologies but also in scalable big data infrastructures that can process high volume and high velocity network traffic. Managers should prioritize systems that support incremental learning and continuous model updating, enabling real time detection of evolving threats such as zero day attacks and advanced persistent threats. By doing so, organizations can significantly reduce response time, improve detection accuracy, and minimize false positives, ultimately enhancing operational efficiency and security resilience.

Second, the study highlights the critical role of organizational readiness, particularly in terms of governance, human resources, and system integration. Managers must ensure that AI driven cybersecurity solutions are aligned with regulatory requirements, risk management frameworks, and internal policies. This includes establishing clear governance structures, ensuring data privacy compliance, and implementing explainable AI mechanisms to enhance trust and accountability. Furthermore, organizations need to invest in workforce development by upskilling cybersecurity professionals to effectively interpret AI generated insights and manage adaptive systems. Without proper human AI collaboration and governance alignment, even the most advanced technological solutions may fail to deliver sustainable value.

Finally, from a strategic perspective, managers should view adaptive cybersecurity not merely as a technical upgrade but as a long term enabler of digital resilience and organizational sustainability. The integration of self learning AI and big data analytics into cybersecurity frameworks supports business continuity, protects critical digital assets, and fosters stakeholder trust in increasingly interconnected digital ecosystems. Managers are encouraged to adopt a proactive and forward looking approach by embedding continuous innovation, scalability planning, and cross functional collaboration into their cybersecurity strategies. This will allow organizations to remain competitive and resilient in the face of rapidly evolving cyber threats while supporting broader digital transformation objectives.

6. CONCLUSION

This study concludes that integrating self learning AI into large scale computer networks provides a resilient and adaptive framework for threat detection in dynamic cybersecurity environments. The findings show that adaptive learning autonomy, distributed scalability, explainability, and governance alignment are key factors influencing the effectiveness of AI driven cybersecurity systems. Unlike conventional static intrusion detection methods, the proposed framework enables continuous adaptation through incremental learning and distributed feedback mechanisms, supporting more responsive and sustainable threat detection. The study also highlights the broader practical value of adaptive AI in strengthening cybersecurity resilience, improving operational efficiency, reducing disruption risks, and supporting reliable decision making in complex enterprise networks. Furthermore, the research aligns with SDGs 9 and SDGs 16 by promoting resilient infrastructure, innovation, secure institutions, accountability, and digital trust through ethically governed AI systems.

In addressing how self learning AI can autonomously detect evolving threats, the study finds that continuous feedback loops, behavioral modeling, and distributed learning are essential for maintaining detection relevance. Learning autonomy reduces reliance on manual retraining and improves responsiveness to new attack patterns. However, limitations exist the qualitative approach limits generalizability, the framework remains conceptual without real world validation, and computational cost trade offs under heavy data loads are not fully explored. Additionally, practical challenges such as resource constraints, infrastructure diversity, and cost implications require further investigation, indicating the need for stronger empirical validation.

Future research should incorporate quantitative or mixed methods to evaluate performance metrics such as detection latency, throughput, and model stability under high data volumes. Testing across diverse network environments, including cloud and edge systems, would improve generalizability. Further studies should also examine real world deployment challenges, including integration complexity and cost. Exploring privacy preserving approaches like federated learning and enhancing transparency through explainable AI are promising directions. Advancing adaptive, scalable, and ethically aligned AI frameworks will be crucial for strengthening digital resilience and supporting sustainable technological development.

7. DECLARATIONS

7.1. About Authors

Dwi Cahyono (DC) https://orcid.org/0000-0001-9951-560X

Herman (HH) https://orcid.org/0000-0001-6818-5142
Ikyboy Van Versie (IV) https://orcid.org/0009-0004-0232-6044

7.2. Author Contributions

Conceptualization: HH; Methodology: DC; Software: IV; Validation: DC and HH; Formal Analysis: IV and DC; Investigation: HH; Resources: DC; Data Curation: IV; Writing Original Draft Preparation: HH and IV; Writing Review and Editing: DC; Visualization: HH and IV; All authors, DC, HH, and IV 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. M. Alnfiai, "Ai-powered cyber resilience: a reinforcement learning approach for automated threat hunting in 5g networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2025, no. 1, p. 68, 2025.

[2] M. A. Hossain, "Deep q-learning intrusion detection system (dq-ids): A novel reinforcement learning approach for adaptive and self-learning cybersecurity," *ICT Express*, 2025.

[3] L. Akoglu and J. Yoo, "Self-supervision for tackling unsupervised anomaly detection: Pitfalls and opportunities," in *2023 IEEE International Conference on Big Data (BigData)*. IEEE, 2023, pp. 1047–1051.

[4] A. Kurniati, "Study of the artificial intelligence role in achieving cybersecurity for critical information infrastructure," *Monas: Jurnal Inovasi Aparatur*, vol. 6, no. 1, pp. 1–10, 2024. [Online]. Available: https://ejournal-bpsdm.jakarta.go.id/index.php/monas/article/view/251

[5] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection," *Information Systems Frontiers*, vol. 25, no. 2, pp. 589–611, 2023.

[6] G. de Carvalho Bertoli, L. A. P. Junior, O. Saotome, and A. L. Dos Santos, "Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach," *Computers & Security*, vol. 127, p. 103106, 2023.

[7] M. Rahmati, "Towards explainable and lightweight ai for real-time cyber threat hunting in edge networks," *arXiv preprint arXiv:2504.16118*, 2025.

[8] M. G. Hardini, N. A. Yusuf, A. R. A. Zahra *et al.*, "Convergence of intelligent networks: Harnessing the power of artificial intelligence and blockchain for future innovations," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 200–209, 2024.

[9] M. Rahmati and A. Pagano, "Federated learning-driven cybersecurity framework for iot networks with privacy preserving and real-time threat detection capabilities," in *Informatics*, vol. 12, no. 3. MDPI, 2025, p. 62.

[10] J. Sivakumar, N. R. Salman, F. R. Salman, H. R. Salimova, and E. Ghimire, "Ai-driven cyber threat detection: enhancing security through intelligent engineering systems," *Journal of Information Systems Engineering and Management*, vol. 10, no. 19, pp. 790–798, 2025.

[11] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.

[12] F. Jemili, K. Jouini, and O. Korbaa, "Intrusion detection based on concept drift detection and online incremental learning," *International Journal of Pervasive Computing and Communications*, vol. 21, no. 1, pp. 81–115, 2025.

[13] M. Siti *et al.*, "Wireless network security design and analysis using wireless intrusion detection system," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 30–39, 2022.

[14] 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.

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

[16] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Explainable artificial intelligence for intrusion detection in iot networks: A deep learning based approach," *Expert Systems with Applications*, vol. 238, p. 121751, 2024.

[17] M. Faisal, S. A. M. Hidayat, A. R. Basrida, M. T. Fazrin *et al.*, "Prototype of water level and rainfall detection system as flood warning based on blynk iot application," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 1–10, 2023.

[18] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 3, 2023.

[19] S. Chitimoju, "Ethical challenges of ai in cybersecurity: bias, privacy, and autonomous decision-making," *Journal of Computational Innovation*, vol. 3, no. 1, 2023.

[20] T. Jiang, G. Shen, C. Guo, Y. Cui, and B. Xie, "Bfls: Blockchain and federated learning for sharing threat detection models as cyber threat intelligence," *Computer Networks*, vol. 224, p. 109604, 2023.

[21] S. Kosasi, U. Rahardja, I. D. A. E. Yuliani, R. Laipaka, B. Susilo, and H. Kikin, "It governance: Performance assessment of maturity levels of rural banking industry," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2022, pp. 1–6.

[22] S. Panda, *Scalable Artificial Intelligence Systems: Cloud-Native, Edge-AI, MLOps, and Governance for Real-World Deployment*. Deep Science Publishing, 2025.

[23] Unknown, "Explainable artificial intelligence for cybersecurity knowledge representation," *Global Science: Journal of Information Technology and Computer Science*, 2026. [Online]. Available: https://garuda.kemdiktisaintek.go.id/journal/view/44820

[24] A. Mohsin, H. Janicke, A. Ibrahim, I. H. Sarker, and S. Camtepe, "A unified framework for human ai collaboration in security operations centers with trusted autonomy," *arXiv preprint arXiv:2505.23397*, 2025.

[25] D. Jonas, N. A. Yusuf, and A. R. A. Zahra, "Enhancing security frameworks with artificial intelligence in cybersecurity," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 83–91, 2023.

[26] D. Cohen, D. Te'eni, I. Yahav, A. Zagalsky, D. Schwartz, G. Silverman, Y. Mann, A. Elalouf, and J. Makowski, "Human–ai enhancement of cyber threat intelligence," *International Journal of Information Security*, vol. 24, no. 2, p. 99, 2025.

[27] S. Tariq, R. Singh, M. B. Chhetri, S. Nepal, and C. Paris, "Bridging expertise gaps: The role of llms in human-ai collaboration for cybersecurity," *arXiv preprint arXiv:2505.03179*, 2025.

[28] Z. Aref, S. Wei, and N. B. Mandayam, "Human-ai collaboration in cloud security: Cognitive hierarchy-driven deep reinforcement learning," *arXiv preprint arXiv:2502.16054*, 2025.

[29] U. Rahardja, V. T. Devana, N. P. L. Santoso, F. P. Oganda, and M. Hardini, "Cybersecurity for fintech on renewable energy from acd countries," in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2022, pp. 1–6.

[30] J. Desikan, S. K. Singh, and A. Jayanthiladevi, "Bachaav: machine learning-augmented human-ai and cryptographic architecture for threat detection in iot-enabled oil and gas industrial networks," *International Journal of Information Technology*, pp. 1–12, 2025.

[31] R. Yaich, A. Balondrade, A. Sicard, C. Fouquiau, G. Giraud, K. Amokrane-Ferka, and E. Arbaretier, "Symbiotic human–ai collaboration for augmented cybersecurity operations," in *Proceedings of the AAAI Symposium Series*, vol. 6, no. 1, 2025, pp. 350–358.

[32] H. Jahani, R. Jain, and D. Ivanov, "Data science and big data analytics: a systematic review of methodologies used in the supply chain and logistics research," *Annals of Operations Research*, vol. 359, no. 2, pp. 1297–1354, 2026.

[33] A. G. Prawiyogi and L. Meria, "For a cps-iot enabled healthcare ecosystem consider cognitive cybersecurity," *International Transactions on Artificial Intelligence*, vol. 2, no. 1, pp. 24–32, 2023.

[34] U. Rahardja, O. Candra, A. K. Tripathi, M. M. A. Zahra, B. S. Bashar, I. Muda, N. K. A. Dwijendra, S. Aravindhan, and R. Sivaraman, "The use of hybrid solar energy to supply electricity to remote areas: Advantages and limitations," *Mathematical Modelling of Engineering Problems*, vol. 10, no. 2, 2023.

[35] L. Theodorakopoulos, A. Theodoropoulou, and C. Klavdianos, "Big data analytics and ai for consumer behavior in digital marketing: Applications, synthetic and dark data, and future directions," *Big Data and Cognitive Computing*, vol. 10, no. 2, p. 46, 2026.

[36] K. Shahzad, S. A. Khan, and A. Iqbal, "Effects of big data analytics on university libraries: A systematic literature review of impact factor articles," *Journal of Librarianship and Information Science*, vol. 58, no. 1, pp. 41–59, 2026.

[37] F. Abdullah, H. M. Naeem, and H. Aslam, "Big data, bigger ideas: the role of big data analytics management capability in supply chain sustainability," *Industrial Management & Data Systems*, vol. 126, no. 3, pp. 922–944, 2026.

[38] L. Meria, "Development of automatic industrial waste detection system for leather products using artificial intelligence," *International Transactions on Artificial Intelligence*, vol. 1, no. 2, pp. 195–204, 2023.

[39] M. Jafari, P. Akhavan, and A. H. Akbari, "Enhancing supply chain agility and performance through big data analytics: the role of digitalization and top management support," *International Journal of Productivity and Performance Management*, pp. 1–22, 2026.

[40] M. A. Rahman, P. Saha, H. Belal, S. Hasan Ratul, and G. Graham, "Big data analytics capability and supply chain sustainability: analyzing the moderating role of green supply chain management practices," *Benchmarking: An International Journal*, vol. 33, no. 2, pp. 417–443, 2026.

[41] Q. Pang, J. Du, M. Fang, and L. Wang, "Strategic mechanism for enhanced sustainable practice performance in shipping organizations through big data analytics powered by artificial intelligence," *Journal of Enterprise Information Management*, vol. 39, no. 1, pp. 188–213, 2026.

[42] N. Lutfiani, D. Apriani, E. A. Nabila, and H. L. Juniar, "Academic certificate fraud detection system framework using blockchain technology," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 55–64, 2022.

[43] M. H. Kabir, M. Razib, Z. Jahin, and Z. Jesan, "Zero trust based critical infrastructure cybersecurity framework with ai-driven threat detection and secure network modernization," *Journal of Computer Science and Technology Studies*, vol. 8, no. 5, pp. 01–14, 2026.

[44] S. R. Jeremiah, A. El Azzaoui, S. Gritzalis, and J. H. Park, "Multi-view learning and model fusion framework for threat detection in multi-protocol iomt networks," *Information Fusion*, vol. 125, p. 103435, 2026.

[45] S. Kumara, "A lightweight deep learning based classification models for non-human identity threat detection," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*. IEEE, 2026, pp. 1–6.

[46] A. Kanivia, H. Hilda, A. Adiwijaya, M. F. Fazri, S. Maulana, and M. Hardini, "The impact of information technology support on the use of e-learning systems at university," *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 122–132, 2024.

[47] N. J. Benfey, F. Cookson, D. Foubert, E. Cianfarano, O. Ruge, A. T. Benfey, A. Schohl, and E. S. Ruthazer, "Norepinephrine acts through radial astrocytes in the developing optic tectum to enhance threat detection and escape behavior," *Cell Reports*, vol. 45, no. 2, 2026.

[48] E. R. Rahayu, A. Aprillia, R. Z. Ikhsan, A. Adiwijaya, and A. Kumara, "Cybersecurity in the age of iot and developing frameworks for securing smart devices and networks," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 46–54, 2025.

[49] M. Alamri, N. Tariq, M. Humayun, and M. Alshammeri, "Energy-efficient threat detection in iot healthcare using ai and blockchain-enhanced fog–cloud architecture," *Cluster Computing*, vol. 29, no. 2, p. 108, 2026.

[50] M. A. Uddin, M. Mahiuddin, and I. H. Sarker, "An explainable transformer-based model for phishing email detection: A large language model approach," *Computer Networks*, p. 112061, 2026.

[51] A. Alageel and S. Maffeis, "Investigation of advanced persistent threats network-based tactics, techniques and procedures," *Computer Networks*, p. 112069, 2026.

[52] S. Watini, Q. Aini, U. Rahardja, N. P. L. Santoso, and D. Apriliasari, "Class dojolms in the interactive learning of paud educators in the disruption era 4.0," *Journal of Innovation in Educational and Cultural Research*, vol. 3, no. 2, pp. 215–225, 2022.