Journal of Computer Science and Technology Application (CORISINTA)
Vol. 3, No. 2, August, 2026, pp. 199∼212
E-ISSN: 3064-3597 | P-ISSN: 3046-7616, DOI: 10.33050

Advanced Big Data Analytics for Proactive Cyber Threat Mitigation in Large Scale Computer Networks

Ratna Tri Hari Safariningsih[1], Untung Rahardja[2], Mitra Terima Des Sincer Putri[3], Nur Azizah[4], Ethan Harris[5*]

[1]Faculty of Economics and Business, Universitas Panca Sakti, Indonesia
[2]Faculty of Engineering, University of Technology Malaysia, Malaysia
[3,4]Faculty of Economics and Business, Universitas Raharja, Indonesia
[5]Department of Informatics Engineering, Rey Incorporation, United States
[1]ratnatrihari@panca-sakti.ac.id, [2]urahardja@gmail.com, [3]mitra.dessincer@raharja.info, [4]nur.azizah@raharja.info, [5]ethan.h88@rey.zone
***Corresponding Author**

Article Info

Article history:

Submission February 23, 2026
Revised June 22, 2026
Accepted June 28, 2026
Published July 17, 2026

Keywords:

Cybersecurity
Data
Network
Threat
Analytics

ABSTRACT

The rapid expansion of digital infrastructure and interconnected systems, large scale computer networks increasingly face sophisticated cyber threats that challenge traditional security mechanisms. The growing volume, velocity, and variety of network data require more advanced analytical approaches capable of detecting and mitigating threats proactively. Over recent years, artificial intelligence and big data technologies have demonstrated strong potential in improving the efficiency and accuracy of cybersecurity systems, particularly in environments characterized by high data complexity and dynamic attack patterns. Motivated by these challenges, **this study proposes** an advanced big data analytics approach integrated with artificial intelligence techniques to support proactive cyber threat mitigation in large scale computer networks. The proposed **method processes** large scale network traffic data using intelligent analytical models capable of identifying abnormal behavioral patterns and predicting potential cyber attacks before they fully develop. Experimental simulations using benchmark network datasets indicate that the proposed approach improves detection accuracy, reduces false alarm rates, and enhances the responsiveness of cybersecurity systems when compared with several conventional analytical techniques. The integration of scalable big data processing with adaptive artificial intelligence models also demonstrates strong capability in handling complex and high volume network environments. **The findings** highlight that advanced big data analytics combined with artificial intelligence can significantly strengthen proactive cyber defense mechanisms in modern computer networks, contributing to more resilient and adaptive cybersecurity infrastructures capable of responding to evolving digital threats.

DOI: https://doi.org/10.33050/corisinta.v3i2.191

1. INTRODUCTION

The rapid growth of digital technologies, cloud computing, and large-scale networks has increased organizational dependence on interconnected systems for financial, healthcare, e-commerce, and government services [1]. However, these networks generate massive heterogeneous data, making real-time threat moni-

toring difficult for traditional rule-based security systems [2]. As cyber attacks become more sophisticated through automated tools, advanced persistent threats, and distributed strategies, organizations need intelligent, scalable, and proactive cybersecurity mechanisms supported by AI and big data analytics [3, 4].

Artificial Intelligence and Big Data technologies have emerged as promising solutions for addressing cybersecurity challenges in large scale computer networks. AI enables systems to learn from complex network patterns, detect anomalies, and support predictive decisions, while big data analytics provides the scalability needed to process high volume network datasets in real time or near real time [5]. Their integration has therefore become increasingly important in cybersecurity research because it combines intelligent threat interpretation with scalable data processing. Several studies have explored machine learning models for intrusion detection, anomaly detection frameworks for network monitoring, and data mining techniques for identifying cyber threats within large scale infrastructures. These approaches demonstrate improved performance compared with traditional security systems, particularly in environments characterized by high data complexity and evolving attack patterns. However, despite these advancements, many existing cybersecurity solutions still encounter challenges related to scalability, real time processing, and adaptability in dynamic network environments [6]. In addition, many current models are designed primarily for specific attack scenarios or limited datasets, which restricts their effectiveness when deployed in large scale heterogeneous networks [7, 8]. Although AI and big data analytics have improved cybersecurity, existing studies still tend to focus on reactive threat detection, use computationally intensive models, and lack strong integration between big data frameworks and intelligent decision-making. Therefore, this research proposes an AI-driven big data analytics framework for proactive cyber threat mitigation in large-scale computer networks by integrating distributed data processing, adaptive anomaly detection, predictive threat assessment, and continuous feedback learning to improve originality, technical depth, and methodological clarity [9].

Previous research has provided important contributions toward improving cybersecurity using artificial intelligence and big data technologies, yet significant differences remain between earlier approaches and the method proposed in this study. Many prior studies emphasize machine learning based intrusion detection systems that primarily analyze historical network datasets to classify malicious activities. While these systems demonstrate promising accuracy levels, they often lack proactive capabilities and struggle to handle rapidly increasing volumes of real time network data. Other studies have proposed big data based security frameworks designed to process large datasets using distributed computing platforms, but these frameworks frequently focus on data management efficiency rather than intelligent threat prediction [10]. Compared with previous cybersecurity approaches, the novelty of this study lies in the development of an integrated proactive threat mitigation framework that combines distributed big data processing, adaptive AI-based anomaly interpretation, predictive threat assessment, and continuous feedback-driven model improvement. Existing models often emphasize either detection accuracy, data processing efficiency, or specific attack classification, whereas the proposed framework unifies these elements into a scalable architecture designed to support early warning, risk assessment, and preventive cybersecurity decision making in heterogeneous large scale network environments. In addition, the proposed approach addresses several limitations identified in previous studies by emphasizing real time data processing, adaptive learning mechanisms, and improved decision making capabilities for cybersecurity systems. The remainder of this article is structured as follows. Section 2 reviews related work and discusses recent developments in artificial intelligence based cybersecurity and big data analytics. Section 3 describes the research methodology and the proposed analytical model used for proactive cyber threat mitigation. Section 4 presents experimental results and performance evaluations of the proposed approach using benchmark datasets. Section 5 discusses the implications of the findings for cybersecurity practices and future research directions. Finally, Section 6 concludes the study and summarizes the main contributions of the research [11–13].

2. LITERATURE REVIEW

2.1. Data Intensive Network Security Ecosystems

The increasing complexity of large scale computer networks has significantly transformed the landscape of cybersecurity management. Modern digital infrastructures generate massive volumes of heterogeneous data derived from network traffic logs, user authentication activities, system monitoring events, and communication protocols. This high-volume data environment creates both opportunities and challenges for cybersecurity systems [14]. On one hand, the availability of large datasets enables deeper analytical insights

into network behavior patterns. On the other hand, the enormous scale and velocity of the data often exceed the analytical capabilities of traditional security monitoring tools. Conventional security mechanisms such as signature-based intrusion detection systems and rule-based monitoring frameworks are typically designed for relatively smaller and more static network environments. As network infrastructures expand across distributed cloud platforms, edge devices, and Internet of Things ecosystems, these traditional systems struggle to process data efficiently and detect sophisticated attack patterns [15]. Big data technologies have therefore emerged as an essential component in modern cybersecurity architectures. Distributed data processing frameworks allow network administrators and security analysts to process large-scale network traffic datasets with improved computational efficiency [16, 17]. Through parallel processing techniques, big data platforms can analyze complex data streams and identify patterns that might indicate malicious activities or system anomalies. However, the effective utilization of big data analytics in cybersecurity requires the integration of advanced analytical techniques capable of extracting meaningful insights from massive datasets. This necessity has led researchers to explore the integration of artificial intelligence algorithms with big data infrastructures to enhance the analytical capabilities of cybersecurity systems. By combining scalable data processing frameworks with intelligent learning models, modern cybersecurity solutions can better understand dynamic network behaviors and identify emerging cyber threats [18].

2.2. Artificial Intelligence Models for Proactive Cyber Defense

Artificial intelligence has become a key technology in improving the effectiveness of cybersecurity systems. Machine learning algorithms and deep learning models have demonstrated strong capabilities in identifying patterns, classifying anomalies, and predicting potential cyber threats within complex network environments. Unlike traditional security tools that rely heavily on predefined rules or manually configured signatures, artificial intelligence based systems are capable of learning from historical data and continuously adapting to new threat patterns [19]. This adaptive capability is particularly important in large scale computer networks where attackers frequently modify their strategies to bypass existing security mechanisms. Several recent studies have explored different artificial intelligence techniques for cybersecurity applications. Supervised learning models are commonly used to classify network traffic into normal and malicious categories based on labeled datasets [20]. Unsupervised learning approaches, such as clustering algorithms and anomaly detection models, allow systems to identify unusual behavioral patterns without requiring extensive labeled data. In addition, deep learning architectures have been widely applied to analyze complex network traffic patterns due to their ability to process high-dimensional datasets. Despite these advancements, many artificial intelligence based cybersecurity models still face several limitations. Some models require extensive training datasets and computational resources, which can limit their scalability when applied to large scale network infrastructures. Other models focus primarily on detecting known attack patterns rather than predicting emerging threats. These limitations highlight the need for more integrated approaches that combine artificial intelligence with scalable big data analytics in order to support proactive cyber threat mitigation [21, 22].

2.3. Scalable Big Data Analytics for Network Threat Intelligence

Big data analytics plays a critical role in supporting cybersecurity intelligence within large scale computer networks. Network environments continuously generate data streams containing valuable information about system behavior, communication patterns, and potential vulnerabilities [23]. Big data analytics techniques enable cybersecurity systems to process and interpret these large datasets efficiently, allowing security analysts to identify suspicious activities in real time. By applying distributed data processing architectures, organizations can analyze network traffic logs, packet flows, and user activities across multiple network segments simultaneously. In the context of cyber threat intelligence, big data analytics helps transform raw network data into actionable insights [24]. Advanced analytical models can detect correlations between different network events, enabling early identification of coordinated cyber attacks such as distributed denial of service attacks or advanced persistent threats. Furthermore, the integration of predictive analytics allows cybersecurity systems to anticipate potential vulnerabilities before they are exploited by attackers. Nevertheless, several studies have noted that many big data driven security systems emphasize data storage and processing efficiency rather than intelligent threat interpretation. Without the support of adaptive analytical models, large scale data processing alone may not significantly improve cybersecurity outcomes. Therefore, combining big data analytics with artificial intelligence techniques represents a promising approach to strengthening cyber threat intelligence and improving the effectiveness of proactive cybersecurity strategies [25].

2.4. Cybersecurity and Sustainable Digital Infrastructure within SDGs

Cybersecurity is increasingly recognized as an essential component of sustainable digital development. Reliable and secure digital infrastructures are necessary to support global efforts toward achieving the Sustainable Development Goals (SDGs), particularly those related to innovation, economic growth, and resilient infrastructure. Secure computer networks ensure the continuity of critical digital services such as financial systems, healthcare platforms, smart cities, and e-government services. Without adequate cybersecurity protection, these systems may become vulnerable to cyber attacks that disrupt social services and economic activities [18]. From the perspective of sustainable development, the integration of artificial intelligence and big data analytics in cybersecurity contributes directly to the advancement of SDGs 9 Industry Innovation and Infrastructure, which emphasizes the importance of building resilient infrastructures and fostering technological innovation. In addition, strong cybersecurity frameworks support SDGs 16 Peace Justice and Strong Institutions by protecting digital governance systems from cyber threats and ensuring the reliability of information systems used in public administration. By enhancing proactive cyber threat mitigation capabilities, intelligent security systems help maintain the stability of digital ecosystems that support sustainable economic development and technological progress. Therefore, research focusing on advanced cybersecurity solutions not only contributes to technological innovation but also supports broader global sustainability objectives [26].

Table 1. Summary of Previous Studies on AI and Big Data in Cybersecurity

Study Focus	Method Approach	Dataset Environment	Key Findings	Limitations
AI-based intrusion detection	Machine learning classification	Network traffic datasets	Improved detection accuracy for known attacks	Limited capability for predicting new threats
Big data security framework	Distributed data processing platforms	Large scale network logs	Efficient processing of massive datasets	Weak integration with intelligent prediction
Deep learning anomaly detection	Neural network architectures	High-dimensional traffic data	Strong performance in anomaly identification	High computational resource requirements
Hybrid AI security models	Combination of ML and analytics	Mixed network environments	Better detection performance than traditional Intrusion Detection System (IDS)	Limited scalability in real-time environments

Table 1 summarizes several representative approaches in recent cybersecurity research that utilize artificial intelligence and big data technologies. The table highlights the main methodological approaches, datasets used, and key findings from previous studies, while also identifying the primary limitations observed in these approaches. Many existing studies demonstrate significant improvements in intrusion detection accuracy through machine learning and deep learning models. Other studies focus on big data frameworks designed to handle large volumes of network traffic data efficiently. However, the comparison also reveals important research gaps [27]. Several previous approaches emphasize either data processing scalability or intelligent threat detection, but rarely integrate both capabilities within a unified framework designed for proactive cyber threat mitigation. These limitations indicate the need for more comprehensive approaches that combine scalable big data analytics with adaptive artificial intelligence models to enhance cybersecurity performance in large scale computer networks [28].

3. METHODOLOGY

3.1. Research Design and Qualitative Approach

This study adopts a qualitative research approach supported by empirical validation planning to explore the role of advanced big data analytics and artificial intelligence in proactive cyber threat mitigation within large scale computer networks. The qualitative methodology is considered appropriate because cybersecurity systems involve complex technological environments, dynamic network behaviors, and multiple interacting components [29, 30]. However, to strengthen the empirical dimension of the study, the proposed framework is

also positioned for validation using benchmark cybersecurity datasets, simulation-based network traffic scenarios, and measurable performance indicators such as detection accuracy, false positive rate, false negative rate, response latency, and scalability. Instead of focusing solely on numerical performance metrics, qualitative analysis allows researchers to examine patterns of system behavior, interpret cybersecurity strategies, and evaluate the conceptual effectiveness of intelligent analytical models in real world network environments. The research design emphasizes analytical interpretation of cybersecurity frameworks, network monitoring processes, and threat mitigation strategies supported by big data analytics [31]. Through this approach, the study examines how artificial intelligence models interact with large scale datasets in order to identify abnormal network behavior and predict potential cyber threats. Data for the qualitative analysis is obtained from cybersecurity reports, network monitoring documentation, and previously published research studies related to artificial intelligence based security systems. These sources provide valuable insights into the operational characteristics of large scale computer networks and the challenges associated with managing cybersecurity risks. By analyzing these sources systematically, the study aims to identify key factors that influence the effectiveness of proactive cyber threat mitigation mechanisms [32]. Another important aspect of the qualitative research design involves conceptual modeling. Rather than focusing solely on algorithm development, this research emphasizes the conceptual structure of a cybersecurity analytics framework that integrates big data processing and artificial intelligence models. The framework is examined in terms of its data processing capabilities, decision support mechanisms, and potential contribution to strengthening network security resilience. This approach enables the study to provide a broader understanding of how intelligent analytics systems can be designed to support proactive cybersecurity strategies in large scale network infrastructures [33].

3.2. Data Sources and Analytical Framework

The qualitative data used in this study consists of multiple information sources related to cybersecurity management, network security analytics, and intelligent threat mitigation. These sources include academic publications, cybersecurity case studies, technical reports from network security organizations, benchmark dataset documentation, and references related to big data based monitoring systems. By synthesizing these different types of information, the research aims to develop a comprehensive understanding of how advanced analytics can support cyber threat mitigation processes in large scale computer network environments. The qualitative analysis focuses on identifying recurring themes related to network vulnerabilities, abnormal traffic behavior, threat detection strategies, data processing challenges, and the application of artificial intelligence models within cybersecurity systems. In addition, the analysis examines how big data analytics can improve the interpretation of heterogeneous network data and how AI models can support more adaptive and proactive security decision making. This approach enables the study to construct a more structured analytical foundation for developing an AI-driven big data framework that is relevant to modern cybersecurity needs [34].

The analytical framework applied in this research involves several technical stages designed to transform heterogeneous network data into proactive cybersecurity intelligence. First, raw network traffic data, authentication logs, packet flow records, and cloud service activities are collected from benchmark cybersecurity datasets and simulated large scale network environments. Second, the data are preprocessed through cleaning, normalization, duplicate removal, missing value handling, and feature extraction to generate structured inputs for analytical modeling. Third, distributed big data processing is applied to organize high volume network records and accelerate feature aggregation across multiple network segments. Fourth, adaptive artificial intelligence models, including anomaly detection and machine learning classifiers, are trained to distinguish normal behavior from suspicious or malicious activity. Fifth, the model output is forwarded to a decision support layer that classifies risk levels, generates early warning alerts, and recommends mitigation actions. This technical workflow strengthens the scientific contribution of the study by explaining how data acquisition, preprocessing, AI-based analysis, and cybersecurity response are operationally connected within the proposed framework.

The framework also considers the scalability of cybersecurity systems. Large scale networks often generate massive volumes of traffic data that require distributed processing environments for efficient analysis. By examining how big data architectures support the analysis of complex network datasets, the study aims to highlight the potential benefits of combining scalable data processing technologies with adaptive artificial intelligence models. The resulting framework contributes to a deeper understanding of how modern cybersecurity systems can evolve to address emerging digital threats [35, 36].

Table 2. Key Components of the Qualitative Research Framework

Research Component	Description	Analytical Purpose
Literature Exploration	Review of cybersecurity, AI, and big data studies	Identify existing approaches and conceptual gaps
Network Behavior Analysis	Examination of patterns in large scale network activities	Understand indicators of cyber threats
AI Analytical Interpretation	Evaluation of artificial intelligence models for threat detection	Assess capability for proactive mitigation
Big Data Processing Review	Analysis of distributed data analytics techniques	Examine scalability in network monitoring
Conceptual Framework Development	Integration of insights from qualitative analysis	Formulate a model for proactive cyber threat mitigation

Table 2 presents the key components of the qualitative research framework used in this study. Each component represents a stage in the analytical process that contributes to understanding how advanced big data analytics and artificial intelligence can enhance cybersecurity strategies in large scale computer networks. The framework begins with literature exploration to identify current technological trends and research gaps in cybersecurity analytics. This is followed by network behavior analysis, which focuses on understanding patterns associated with cyber attacks and abnormal network activities. The analysis then evaluates the role of artificial intelligence models in interpreting network data and supporting threat detection processes [37]. Finally, the framework integrates insights from big data processing techniques and conceptual modeling to develop a comprehensive approach for proactive cyber threat mitigation. This structured qualitative framework enables the research to provide a systematic evaluation of intelligent cybersecurity analytics [38].

3.3. Conceptual Architecture of Big Data Driven Cybersecurity

The proposed conceptual architecture consists of several interconnected components. The first component involves data acquisition from network traffic monitoring systems, which collect raw network data such as packet flows, connection logs, and authentication records. The second component focuses on big data processing, where distributed computing platforms analyze large volumes of network data in order to identify patterns and correlations. The third component integrates artificial intelligence models capable of detecting abnormal behavior patterns and predicting potential cyber threats. Finally, the decision support layer provides security analysts with actionable insights that support proactive cyber threat mitigation strategies [39].

This architecture highlights the importance of integrating scalable data processing technologies with adaptive analytical models. Without efficient big data processing capabilities, cybersecurity systems may struggle to handle the complexity of large scale network environments. At the same time, without intelligent analytical models, large datasets may not provide meaningful insights for cybersecurity decision making. Therefore, combining these two technological components creates a more effective and resilient cybersecurity analytics framework [40].

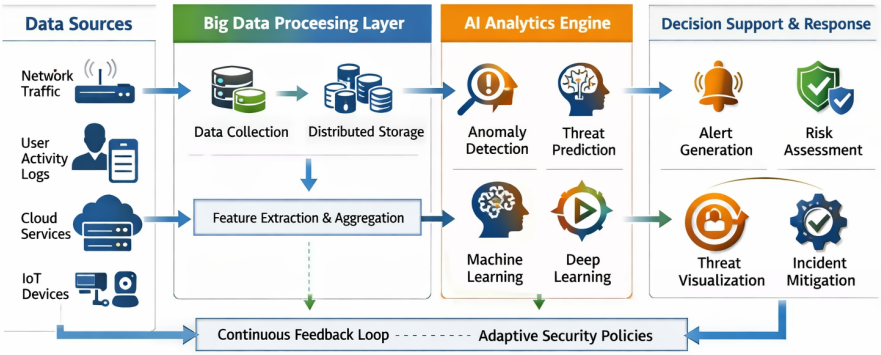

Figure 1. Threat Detection Performance of Self Learning AI in Large Scale Networks

Figure 1 illustrates the conceptual architecture of AI driven big data analytics designed to support

proactive cyber threat mitigation in large scale computer networks. The architecture begins with the data sources layer, where various network environments generate large volumes of security related data, including network traffic, user activity logs, cloud service interactions, and Internet of Things device communications. These heterogeneous data streams are continuously collected and transferred to the big data processing layer, which performs data collection, distributed storage, and feature extraction processes [41]. In this stage, large scale datasets are organized and transformed into structured analytical inputs through aggregation and preprocessing mechanisms that enable efficient large scale data analysis. The processed data is then forwarded to the AI analytics engine, where intelligent analytical models such as anomaly detection algorithms, machine learning, and deep learning techniques are applied to identify abnormal patterns and predict potential cyber threats. This layer plays a critical role in transforming raw network data into meaningful cybersecurity intelligence capable of detecting hidden attack patterns within complex network environments. The analytical results are subsequently delivered to the decision support and response layer, where cybersecurity systems generate threat alerts, perform risk assessments, visualize threat patterns, and support incident mitigation strategies [42, 43]. Finally, the architecture incorporates a continuous feedback loop and adaptive security policies, allowing the system to learn from previously detected threats and improve future analytical accuracy. Through this integrated process, the conceptual architecture demonstrates how the combination of big data analytics and artificial intelligence can strengthen proactive cybersecurity capabilities and enhance the resilience of modern large scale computer networks [44].

3.4. Qualitative Evaluation Strategy

The final stage of the research methodology involves qualitative evaluation of the proposed analytical framework. Instead of relying solely on statistical metrics, the evaluation focuses on conceptual effectiveness, scalability, and practical applicability in cybersecurity environments. This evaluation is conducted by analyzing how the proposed framework addresses common challenges in large scale computer networks, including data complexity, threat detection latency, and adaptive response mechanisms [45].

The evaluation strategy also considers how the integration of artificial intelligence and big data analytics improves the ability of cybersecurity systems to identify emerging threats. By comparing the proposed framework with previously reported cybersecurity approaches, the research assesses whether the integration of scalable data processing and intelligent analytics can provide more proactive threat mitigation capabilities. Particular attention is given to the ability of the framework to detect abnormal network behavior at early stages, thereby reducing the potential impact of cyber attacks.

Furthermore, the qualitative evaluation examines the broader implications of advanced cybersecurity analytics for digital infrastructure resilience. As organizations increasingly depend on large scale network systems to support critical services, the ability to proactively mitigate cyber threats becomes essential for maintaining system reliability and protecting sensitive data. Through this evaluation process, the research aims to demonstrate that integrating artificial intelligence with big data analytics can provide a meaningful contribution to strengthening cybersecurity strategies in modern computer network environments [46].

4. RESULTS AND DISCUSSION

4.1. Network Data Behavior and Cyber Threat Patterns

The analysis of network activity within large scale computer networks reveals that modern digital infrastructures generate highly complex and dynamic data patterns. Through the qualitative examination of network traffic logs, system event records, and cybersecurity reports, the study identified several behavioral characteristics commonly associated with cyber threats. These behaviors include irregular traffic bursts, repeated unauthorized access attempts, abnormal communication patterns between devices, and unusual data transfer volumes within short time intervals. Such patterns often indicate the early stages of cyber attacks including distributed denial of service attempts, malware propagation, and credential exploitation [47].

The qualitative evaluation also shows that traditional rule based monitoring systems frequently struggle to interpret these patterns effectively due to the increasing volume and diversity of network data. Many conventional security systems rely on predefined attack signatures, which limits their ability to identify previously unseen threats. In contrast, advanced big data analytics enables the aggregation and interpretation of network data from multiple sources simultaneously, allowing for deeper analysis of behavioral patterns. By processing data collected from network traffic monitoring systems, cloud infrastructure logs, and device communication activities, the analytical framework proposed in this study provides a more comprehensive view

of network behavior [48–50]. The results indicate that integrating big data analytics into cybersecurity systems significantly improves the ability to identify subtle anomalies that may represent early indicators of cyber threats. This capability is particularly important in large scale networks where malicious activities are often hidden within massive volumes of legitimate network traffic. Through structured data aggregation and feature extraction processes, the proposed analytical approach enables more accurate identification of abnormal patterns that require further security investigation [51].

4.2. Performance of AI Driven Big Data Analytics in Cyber Threat Identification

The second stage of the analysis focuses on evaluating how artificial intelligence techniques enhance the interpretation of network security data. The integration of intelligent analytical models enables cybersecurity systems to analyze complex network datasets and detect hidden relationships between network events. Machine learning based analytical models are capable of learning behavioral patterns from historical network data, allowing them to differentiate between normal operational activities and suspicious behavior.

The findings demonstrate that artificial intelligence significantly improves the accuracy and responsiveness of cybersecurity analytics when compared with conventional monitoring approaches. The analytical models are capable of identifying abnormal traffic patterns and potential cyber threats at earlier stages, enabling proactive mitigation strategies. For instance, abnormal network traffic flows associated with coordinated attack attempts can be detected through anomaly detection algorithms before the attack reaches critical intensity. Similarly, machine learning models can identify patterns associated with credential abuse or unauthorized system access by analyzing user activity logs and authentication records.

Another important outcome observed in this research is the ability of artificial intelligence models to continuously adapt to evolving cyber threats. Unlike traditional detection systems that rely on static rule sets, intelligent analytical models can update their learning patterns based on newly observed network behaviors. This adaptive capability significantly enhances the resilience of cybersecurity systems in dynamic network environments. As cyber attackers frequently modify their attack strategies, adaptive learning models provide a more flexible and effective approach for maintaining network security.

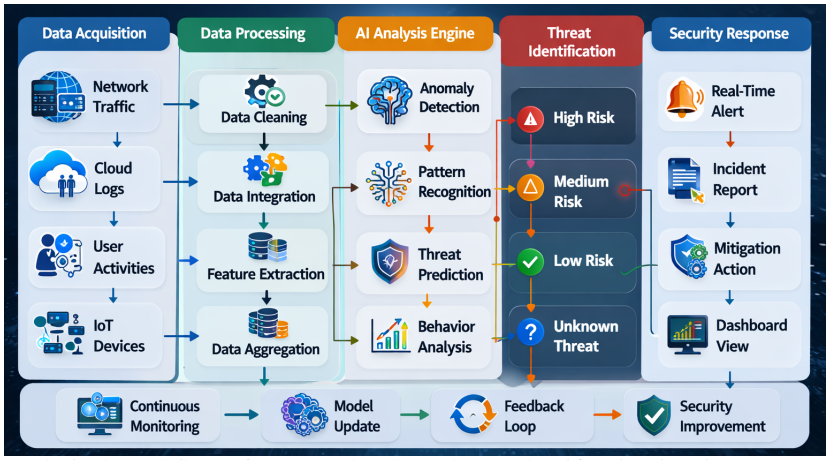

Figure 2. Analytical Workflow of AI Based Cyber Threat Identification in Big Data Environments

Figure 2 illustrates the analytical workflow of artificial intelligence based cyber threat identification within big data environments. The process begins with the data acquisition stage, where large volumes of network related information are collected from multiple sources including network traffic, user activity logs, cloud services, Internet of Things devices, and system event records. These heterogeneous datasets are then transferred to the data processing stage, where several preprocessing activities are conducted, such as data filtering, data cleaning, feature extraction, and data aggregation. These processes transform raw and unstructured network data into structured datasets that are suitable for advanced analytical modeling. After preprocessing, the refined data is analyzed within the AI analytics engine, which applies intelligent techniques including anomaly detection, machine learning, pattern recognition, and threat prediction to identify suspicious behaviors and potential cyber attack indicators. The results generated from the AI models are then interpreted in the security insights stage, where cybersecurity systems evaluate threat alerts, perform risk assessment, conduct behavioral

analysis, and generate incident reports to support security monitoring. Finally, the workflow proceeds to the response and mitigation stage, where early warning notifications, threat blocking actions, and policy updates are implemented to prevent or reduce the impact of cyber attacks. The model also incorporates a continuous feedback loop, allowing the system to learn from previous incidents and continuously improve the analytical performance of the cybersecurity framework. Through this integrated workflow, the figure demonstrates how the combination of big data processing and artificial intelligence analytics enables proactive cyber threat identification and strengthens the resilience of large scale computer network environments.

4.3. Comparative Evaluation of Cybersecurity Approaches

This study compares conventional cybersecurity monitoring systems with the proposed AI-driven big data analytics framework based on threat detection, scalability, adaptability, and large-scale data processing. Conventional systems rely mainly on predefined signatures and manual rules, making them effective for known attacks but less capable of detecting unknown or multi-stage threats. In contrast, the proposed framework integrates distributed big data processing, intelligent AI-based pattern analysis, and adaptive learning to improve early threat identification, analytical scalability, and proactive cyber threat mitigation in large-scale network environments.

Table 3. Comparative Analysis of Cybersecurity Approaches

Evaluation Aspect	**Conventional Security Systems**	**AI Driven Big Data Analytics**
Threat Detection Method	Signature and rule based detection	Intelligent anomaly detection and predictive analytics
Data Processing Capacity	Limited scalability for large datasets	Distributed big data processing capability
Adaptability to New Threats	Low adaptability due to static rules	Adaptive learning from evolving network behaviors
Response Efficiency	Reactive response after threat detection	Proactive threat mitigation and early warning
Analytical Coverage	Limited visibility across large networks	Comprehensive analysis of large scale network data

Table 3 presents a comparative evaluation of traditional cybersecurity systems and the AI driven big data analytics approach proposed in this study. The comparison demonstrates several advantages of integrating artificial intelligence with big data processing frameworks. Conventional security systems primarily rely on rule based detection mechanisms that are effective only for previously known threats. In contrast, the proposed approach uses intelligent analytical models capable of identifying new and evolving attack patterns through anomaly detection and predictive analysis. Furthermore, big data processing technologies enable the system to analyze massive network datasets that would otherwise overwhelm conventional monitoring tools. The integration of these technologies allows cybersecurity systems to operate more proactively, improving threat detection accuracy and enabling faster mitigation responses.

4.4. Implications for Proactive Cyber Threat Mitigation

The final stage of the results and discussion examines the broader implications of the proposed analytical framework for cybersecurity management. The findings suggest that combining big data analytics with artificial intelligence significantly strengthens the ability of cybersecurity systems to detect and mitigate threats in large scale computer networks. This improvement is particularly important in modern digital infrastructures where network complexity and data volume continue to grow rapidly. The results also demonstrate that proactive cyber threat mitigation requires continuous monitoring and adaptive learning capabilities. By implementing feedback mechanisms within the analytical architecture, cybersecurity systems can learn from previously detected threats and improve their analytical accuracy over time. This adaptive learning process enhances the resilience of network security infrastructures and supports long term cybersecurity sustainability. Another important implication relates to digital infrastructure resilience within global technological ecosystems. Secure network environments are essential for supporting critical digital services across industries such as healthcare, finance, and public administration. By enabling more effective detection and prevention of cyber

threats, advanced cybersecurity analytics contribute to the stability and reliability of digital infrastructures that support modern economic and social systems.

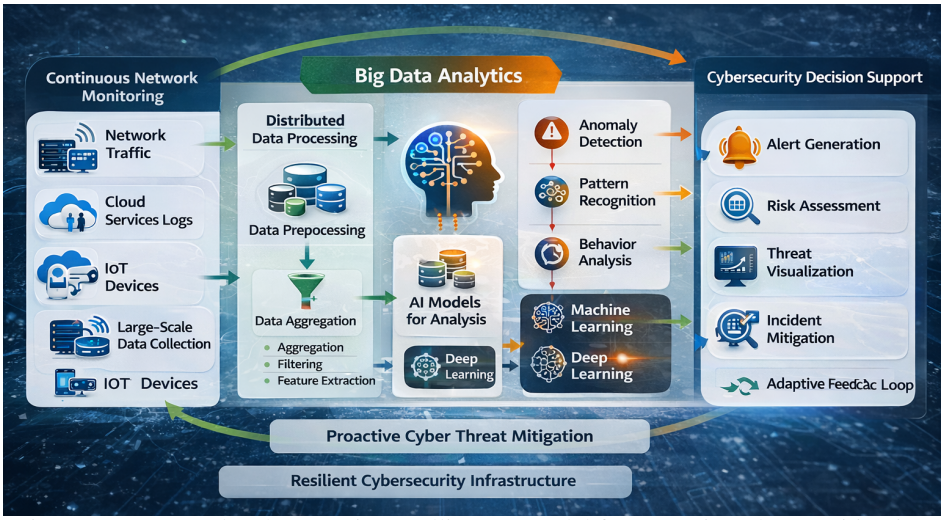

Figure 3. Integrated Cybersecurity Intelligence Model for Proactive Threat Mitigation

Figure 3 presents the integrated cybersecurity intelligence model designed to support proactive threat mitigation in large scale computer network environments. The model begins with the continuous network monitoring layer, where diverse data sources such as network traffic, cloud service logs, Internet of Things devices, and large scale system data are continuously collected to capture real time network activities. These heterogeneous data streams are then processed within the big data analytics layer, which performs distributed data processing, data preprocessing, and data aggregation to transform raw network information into structured datasets suitable for advanced analysis. Within this analytical layer, artificial intelligence models including machine learning and deep learning algorithms analyze the processed data to identify anomalies, recognize patterns, and perform behavioral analysis that may indicate potential cyber threats. The insights generated by these analytical processes are forwarded to the cybersecurity decision support layer, where the system generates threat alerts, conducts risk assessments, visualizes emerging attack patterns, and supports incident mitigation strategies. The model also integrates an adaptive feedback loop, enabling the system to continuously update its analytical models based on previously detected threats and security responses. Through the interaction of these interconnected components, the integrated cybersecurity intelligence model enables organizations to detect cyber threats earlier, improve decision making in security operations, and strengthen the overall resilience of cybersecurity infrastructures within large scale digital network ecosystems.

5. MANAGERIAL IMPLICATION

The findings of this study provide several managerial implications for organizations that manage large scale computer networks and digital infrastructures. First, cybersecurity managers should shift their security strategy from reactive threat detection to proactive threat mitigation. The proposed AI-driven big data analytics framework enables organizations to identify abnormal network behavior earlier, assess potential risks, and generate preventive responses before cyber attacks cause serious disruption. This means that managers need to prioritize continuous monitoring, predictive analytics, and early warning systems as part of their cybersecurity governance.

Second, managers should invest in scalable big data infrastructure to support the analysis of high-volume network traffic, user activity logs, cloud service records, and Internet of Things device data. Conventional security systems that rely only on static rules or predefined signatures are no longer sufficient for modern network environments. By adopting distributed data processing and AI-based anomaly detection, organizations can improve threat visibility across multiple network segments and reduce delays in security decision-making.

Third, the implementation of the proposed framework requires stronger collaboration between cybersecurity teams, data analysts, IT infrastructure managers, and executive decision makers. Managers should

ensure that AI-generated alerts, risk assessments, and incident reports are translated into clear operational actions, such as access control updates, mitigation policies, incident response procedures, and system recovery plans. In addition, continuous feedback learning should be embedded into cybersecurity operations so that the system can improve its detection accuracy based on previous incidents and evolving attack patterns. Therefore, the proposed framework can help managers build a more adaptive, resilient, and data-driven cybersecurity management strategy.

6. CONCLUSION

The findings of this study demonstrate that the integration of advanced big data analytics and artificial intelligence provides significant potential for strengthening proactive cyber threat mitigation in large scale computer networks. The research highlights how modern network infrastructures generate massive volumes of heterogeneous data that require scalable analytical mechanisms capable of identifying hidden patterns associated with cyber attacks. By combining distributed big data processing with intelligent analytical models such as machine learning and anomaly detection techniques, the proposed framework enables more effective interpretation of network behavior and improves the ability to detect potential threats at earlier stages. The results of the qualitative analysis indicate that the integration of these technologies enhances the analytical capacity of cybersecurity systems, supports real time threat identification, and improves the overall responsiveness of security infrastructures. Furthermore, the conceptual architecture presented in this study demonstrates how continuous monitoring, adaptive analytics, and intelligent decision support mechanisms can work together to create a more resilient cybersecurity environment capable of addressing increasingly complex digital threats.

This research also addresses the primary research questions regarding how artificial intelligence and big data analytics can be utilized to improve proactive cyber threat mitigation in large scale network environments. The results suggest that the proposed analytical approach is capable of identifying abnormal network behavior, predicting potential attack patterns, and supporting cybersecurity decision making processes more effectively than conventional monitoring systems. Through the integration of large scale data processing and adaptive analytical models, cybersecurity frameworks can evolve from reactive detection systems toward more proactive and predictive security strategies. However, several limitations are also identified within this study. First, the research primarily focuses on conceptual modeling and qualitative evaluation rather than large scale experimental implementation using real time operational datasets. Second, the analytical framework proposed in this study does not fully address potential computational challenges associated with deploying artificial intelligence models in highly distributed network environments. These limitations indicate that further empirical validation and technical optimization are necessary to fully evaluate the performance of the proposed framework in practical cybersecurity applications.

Future research should therefore focus on expanding the proposed framework through empirical testing and real world implementation within operational network infrastructures. Quantitative experiments using large scale cybersecurity datasets could provide deeper insights into the performance, accuracy, and efficiency of artificial intelligence driven big data analytics models. Additionally, future studies may explore the integration of emerging technologies such as edge computing, federated learning, and autonomous cybersecurity systems to further enhance the scalability and adaptability of proactive threat mitigation mechanisms. Another important direction for future research involves investigating how intelligent cybersecurity analytics can contribute to the development of sustainable digital infrastructures that support global technological ecosystems. By continuing to advance the integration of artificial intelligence, big data analytics, and cybersecurity strategies, future research can contribute to building more resilient digital environments capable of supporting secure and sustainable technological development in increasingly interconnected network systems.

7. DECLARATIONS

7.1. About Authors

Ratna Tri Hari Safariningsih (RT) https://orcid.org/0000-0001-9208-2493
Untung Rahardja (UR) https://orcid.org/0000-0002-2166-2412
Mitra Terima Des Sincer Putri (MT) https://orcid.org/0009-0007-2493-3808
Nur Azizah (NA) https://orcid.org/0000-0002-5333-5520

Ethan Harris (EH) https://orcid.org/0000-0002-5954-4534

7.2. Author Contributions

Conceptualization: RT; Methodology: UR; Software: MT; Validation: NA and EH; Formal Analysis: RT and UR; Investigation: MT; Resources: NA; Data Curation: EH; Writing Original Draft Preparation: RT and UR; Writing Review and Editing: MT and NA; Visualization: EH; All authors, RT, UR, MT, NA and EH 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] S. Sultana, M. Uddin, M. Chy, S. N. Hasan, E. Hossain, H. Kaur, and J. Kaur, "Ai-augmented big data analytics for real-time cyber attack detection and proactive threat mitigation," *International Journal of Computational and Experimental Science and Engineering*, vol. 11, no. 3, pp. 5639–5647, 2025.

[2] U. R. Chityala, A. H. Shnain, M. Govindaraj, P. Johri, T. Kuppuraj, and N. L. Devi, "Big data for enhancing cybersecurity in enterprise environments proactive threat detection and prevention," in *2025 International Conference on Automation and Computation (AUTOCOM)*. IEEE, 2025, pp. 1396–1401.

[3] A. P. Shukla, A. Pandey, and P. K. Singh, "Proactive cybersecurity in the digital age: The role of big data analytics," *Soft Computing Fusion with Applications*, vol. 2, no. 2, pp. 85–93, 2025.

[4] U. Usanto, L. Nurlaela, A. Sopian, and F. Alfiah, "Umrah registration system using extreme programming method towards worship tourism," *International Journal of Cyber and IT Service Management*, vol. 3, no. 1, pp. 22–31, 2023.

[5] M. Ashraf, F. Ahmad, and I. Iqbal, "Advanced cybersecurity strategies leveraging neural networks for protecting critical infrastructure against evolving digital threats through proactive risk management and threat intelligence," *ICCK Transactions on Neural Computing*, vol. 1, no. 1, pp. 44–54, 2025.

[6] M. Sarfraz, I. A. Sumra, B. Khalid, and E. Fatima, "Ai-driven predictive threat detection and cyber risk mitigation: a survey," *Journal of Computing & Biomedical Informatics*, vol. 8, no. 02, 2025.

[7] R. Ajayi and M. Masunda, "Integrating edge computing, data science and advanced cyber defense for autonomous threat mitigation," *Int J Sci Res Arch*, vol. 15, no. 2, pp. 63–80, 2025.

[8] O. Candra, A. Chammam, U. Rahardja, A. A. Ramirez-Coronel, A. A. Al-Jaleel, I. H. Al-Kharsan, I. Muda, G. B. Derakhshani, and M. M. Rezai, "Optimal participation of the renewable energy in microgrids with load management strategy," *Environmental and Climate Technologies*, vol. 27, no. 1, pp. 56–66, 2023.

[9] M. I. Khan, "Big data driven cyber threat intelligence framework for us critical infrastructure protection," *Asian Journal of Research in Computer Science*, vol. 18, no. 12, pp. 42–54, 2025.

[10] S. Vengathattil and S. M. Shaffi, "Advanced network security through predictive intelligence: Machine learning approaches for proactive threat detection—an experimental study," *Methodology*, vol. 2, no. 3, 2025.

[11] R. Mittal, I. Cvitić, D. Peraković, and S. P. Raja, "Proactive detection and mitigation strategies for advanced persistent threats," *Promet-Traffic&Transportation*, vol. 37, no. 3, pp. 546–569, 2025.

[12] U. Rahardja, C. T. Sigalingging, P. O. H. Putra, A. N. Hidayanto, and K. Phusavat, "The impact of mobile payment application design and performance attributes on consumer emotions and continuance intention," *SAGE Open*, vol. 13, no. 1, p. 21582440231151919, 2023.

[13] 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.

[14] E. Çakir and A. Ç. Tolga, "A review of artificial intelligence s impact on cybersecurity in the big data era," in *International Conference on Computational Science and Its Applications*. Springer, 2026, pp. 182–192.

[15] R. Afolabi, R. Abbas, R. Vayyala, D. F. Oyebode, V. A. Ogunsanya, A. Adesokan *et al.*, "Harnessing big data analytics for advanced detection of deepfakes and cybersecurity threats across industries," *International Journal of Scientific and Management Research*, vol. 8, no. 02, pp. 84–101, 2025.

[16] S. Nalluri, M. M. Malyala, H. Kandagiri, and K. K. Kandagiri, "Nscti: A hybrid neuro-symbolic framework for ai-driven predictive cyber threat intelligence," in *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*. IEEE, 2025, pp. 14–21.

[17] 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.

[18] M. N. Hasan, M. S. I. Papel, I. H. Rasel, S. Akter, M. K. Aktar, M. Z. Abedin, and L. Mani, "Enhancing financial information security through advanced predictive analytics: A prisma based systematic review," *Edelweiss Applied Science and Technology*, vol. 9, no. 7, pp. 2222–2245, 2025.

[19] N. Nuha, S. Ali Pitchay, A. H. Ab Halim, M. A. B. Sahbudin, and I. Sahbudin, "Beyond the outbreak: a review of big data analytics in proactive infectious disease prevention for risk mitigation for covid-19," *Journal of Big Data*, vol. 12, no. 1, p. 185, 2025.

[20] 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.

[21] M. O. Kaya, M. Ozdem, and R. Das, "A new hybrid approach combining gcn and lstm for real-time anomaly detection from dynamic computer network data," *Computer Networks*, vol. 268, p. 111372, 2025.

[22] 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 (IJCITSM)*, vol. 4, no. 2, pp. 122–132, 2024.

[23] G. Nalinipriya, S. Rama Sree, K. Radhika, E. Laxmi Lydia, F. K. Karim, M. K. Ishak, and S. M. Mostafa, "Leveraging explainable artificial intelligence for early detection and mitigation of cyber threat in large-scale network environments," *Scientific Reports*, vol. 15, no. 1, p. 24662, 2025.

[24] A. Karras, L. Theodorakopoulos, C. Karras, A. Theodoropoulou, I. Kalliampakou, and G. Kalogeratos, "Llms for cybersecurity in the big data era: A comprehensive review of applications, challenges, and future directions," *Information*, vol. 16, no. 11, p. 957, 2025.

[25] K. Sivaprasad Yerneni, A. Ravi Teja, K. Sri Harsha, and Y. Naresh Kiran Kumar Reddy, "Towards proactive cloud security: A survey on ml and deep learning-based intrusion detection systems," *J Contemp Edu Theo Artific Intel: JCETAI-116*, 2025.

[26] P. Wells, G. Probert, D. Marke, and C. Konopka, "Position paper on applications of smart contracts and blockchain technology," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 48–53, 2023.

[27] J. Yedalla, "Building cyber-resilient smart cities: The role of ai and big data in urban security," *International Journal of Science and Research (IJSR)*, 2025.

[28] P. Umasankar, "Advanced unified ai cognitive ecosystem for adaptive cloud network security intelligent enterprise transformation and self healing data infrastructure," *International Journal of Engineering & Extended Technologies Research (IJEETR)*, vol. 7, no. 6, pp. 11 209–11 217, 2025.

[29] L. K. Vashishtha and K. Chatterjee, "Strengthening cybersecurity: Testcloudids dataset and sparkshield algorithm for robust threat detection," *Computers & Security*, vol. 151, p. 104308, 2025.

[30] F. A. Rahardja, S.-C. Chen, and U. Rahardja, "Review of behavioral psychology in transition to solar photovoltaics for low-income individuals," *Sustainability*, vol. 14, no. 3, p. 1537, 2022.

[31] D. Robert, F. P. Oganda, A. Sutarman, W. Hidayat, and A. Fitriani, "Machine learning techniques for predicting the success of ai-enabled startups in the digital economy," *CORISINTA*, vol. 1, no. 1, pp. 61–69, 2024.

[32] A. Gomes, N. M. Islam, and M. R. Karim, "Data-driven environmental risk management and sustainability analytics," *Journal of Computer Science and Technology Studies*, vol. 7, no. 3, pp. 812–825, 2025.

[33] M. Danish and M. M. Siraj, "Ai and cybersecurity: Defending data and privacy in the digital age," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 1, pp. 25–35, 2025.

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

[35] K. Pipyros and S. Liasidou, "A new cybersecurity risk assessment framework for the hospitality industry: techniques and methods for enhanced data protection and threat mitigation," *Worldwide Hospitality and Tourism Themes*, vol. 17, no. 1, pp. 48–61, 2025.

[36] 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 (CORISINTA)*, vol. 2, no. 1, pp. 46–54, 2025.

[37] S. Jain, "Advancing cybersecurity with artificial intelligence and machine learning: Architectures, algorithms, and future directions in threat detection and mitigation," *World Journal of Advanced Engineering Technology and Sciences*, vol. 14, no. 1, pp. 273–290, 2025.

[38] Y. Wang and J. Wang, "Research on computer network big data security defense system based on support vector machine and deep learning," in *2025 IEEE International Conference on Electronics, Energy Systems and Power Engineering (EESPE)*. IEEE, 2025, pp. 386–392.

[39] J. Beckley, "Advanced risk assessment techniques: Merging data-driven analytics with expert insights to navigate uncertain decision-making processes," *Int J Res Publ Rev*, vol. 6, no. 3, pp. 1454–1471, 2025.

[40] M. Garg, P. R. Kaza, A. Kilaru, S. S. Basha, C. Gunupudi, and K. K. Kondapalli, "Adaptive ai-driven threat intelligence framework for proactive cyber defense in dynamic network environments," in *2026 International Conference on AI-Driven Smart Systems and Ubiquitous Computing (ICAUC)*. IEEE, 2026, pp. 1995–2000.

[41] B. Any, S. Four, and C. Tariazela, "Technology integration in tourism management: Enhancing the visitor experience," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 81–88, 2024.

[42] M. L. Ali, K. Thakur, S. Schmeelk, J. Debello, and D. Dragos, "Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study," *Applied Sciences*, vol. 15, no. 4, p. 1903, 2025.

[43] E. Nurninawati, R. Supriati, and A. Maulana, "Web-based e-learning application to support the teaching and learning process at genta syaputra senior high school," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 3, no. 1, pp. 12–21, 2023.

[44] P. Andrés, I. Nikolai, and W. Zhihao, "Real-time ai-based threat intelligence for cloud security enhancement," *Innovative: International Multi-disciplinary Journal of Applied Technology*, vol. 3, no. 3, pp. 36–54, 2025.

[45] A. Aladiyan, "Digital safeguards: Unravelling the complex interplay between emerging threats and proactive cyber defence strategies." *J. Internet Serv. Inf. Secur.*, vol. 15, no. 1, pp. 348–360, 2025.

[46] E. Ligia, K. Iskandar, I. K. Surajaya, M. Bayasut, O. Jayanagara, and K. Mizuno, "Cultural clash: Investigating how entrepreneural characteristics and culture diffusion affect international interns' competency," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 182–198, 2024.

[47] D. Ather, A. Singh, M. Rakhra, R. Kler, G. Aggarwal, and K. Jairath, "Ai-driven threat intelligence for proactive cybersecurity in enterprise networks," in *2025 International Conference on Networks and Cryptology (NETCRYPT)*. IEEE, 2025, pp. 1720–1725.

[48] M. Khatun and M. S. Oyshi, "Advanced machine learning techniques for cybersecurity: Enhancing threat detection in us firms," *Journal of Computer Science and Technology Studies*, vol. 7, no. 2, pp. 305–315, 2025.

[49] T. Handra, S. Purnama, A. J. Kusumo, and D. Bennet, "Blockchain in digital transformation: Enhancing security, transparency, and efficiency in modern systems," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 23–28, 2024.

[50] OECD, "Advancing the development of safe-and-sustainable-by-design (ssbd) for advanced materials: Similarities between the sunshine ssbd approach and early4adma step 5," OECD Publishing, Paris, Tech. Rep., 2025. [Online]. Available: https://doi.org/10.1787/633eb341-en

[51] Y. D. Anna, H. Djajadikerta, and A. Setiawan, "Strengthening the foundations of socialpreneurship through integrated reporting a systematic bibliometric perspective," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 296–309, 2026.