Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th June 2025. Vol. 4. No. 3; e-ISSN: 2808-4519

Intrusion Detection System Analysis to Improve Computer Network Security

Barlyan Kurdianto[1], Yohanzah Febriyanto[2], Yustian Servanda[3]

[1,2,3] *Department of Information Technology, Faculty of Computers, Mulia University of Balikpapan*
Jl. Letjen Zaini AM No. 9 Damai Bahagia, South Balikpapan, Balikpapan, 76114
barlyankurdianto@outlook.com/barlyankudianto@students.universitasmulia.ac.id[1*],
yohanzahfebri@students.universitasmulia.ac.id[2], yustians@universitasmulia.ac.id[3]

Abstract

This study analyzes intrusion detection systems (IDS) as a vital component in the security of modern computer networks that face increasingly complex cyber threats. Through the Systematic Literature Review approach of 478 publications during 2019-2024, it was found that the CNN-LSTM hybrid model achieved a detection accuracy of 97.3% on the NSL-KDD dataset, far surpassing conventional signature-based methods. The implementation of anomaly-based IDS on Indonesian government infrastructure has identified 45% of attacks that are not detected by traditional solutions, with a reduction in incident response time from 24 hours to 3.5 hours. Federated learning technology for heterogeneous IoT environments increases detection accuracy by 18.7% while reducing network load by up to 76%, while integration with blockchain reduces incident investigation time by 67%. Explainable AI-based frameworks increase security team confidence by 43% and reduce alert fatigue by 38%. The reinforcement learning-based IDS system showed autonomous adaptability with an increase in F1-score from 0.87 to 0.96 without manual intervention. The cost-benefit analysis shows a positive return on Security Investment with an average breakeven point achieved in 14-19 months. This research provides the foundation for the development of an adaptive, contextual, and integrated intrusion detection system to deal with the evolution of contemporary cyber threats.

Keywords: *Intrusion detection systems, network security, artificial intelligence, machine learning, cybersecurity*

1. Introduction

The development of information and communication technology has fundamentally changed the paradigm of using computer networks [1]. In this era of digital transformation, the exchange of data and information through computer networks is the backbone for the operations of various sectors, ranging from educational institutions, government agencies, to multinational companies. This increased reliance on computer networks is directly proportional to the increase in increasingly sophisticated and complex cybersecurity threats. Based on a global cybersecurity report released by Check Point Research in early 2024, there has been a 38% increase in cyberattacks globally compared to the previous year. In Indonesia alone, the State Cyber and Cryptography Agency (BSSN) recorded more than 1.4 million cyberattacks during 2023, with 70% of them targeting computer network infrastructure. Common forms of attacks include Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), SQL Injection, and various types of malware such as ransomware and spyware that are increasingly up-to-date.

Attacks on computer networks have the potential to have significant impacts, ranging from sensitive data leaks, financial losses, to the shutdown of critical services [2]. Organizations such as healthcare providers, banking, and critical infrastructure are prime targets because they have high-value information assets. According to a recent study from IBM Security, the average cost to address the impact of a data security breach reached US$4.45 million per incident in 2023. In an effort to anticipate and address these threats, the Intrusion Detection System (IDS) is a vital component in modern network security architectures. IDS serves as a surveillance system that can detect suspicious activity or security policy violations on networks and computer systems. The development of IDS technology has evolved from a conventional signature-based approach to a more adaptive system by utilizing artificial intelligence and machine learning.

The accelerated digital transformation due to the COVID-19 pandemic has created a drastic expansion of the attack surface for organizations around the world [3]. Remote and hybrid work policies have resulted in a significant increase in the number of devices connected to the company's network through various access points that are often not well controlled. According to a report from Cybersecurity Ventures, global losses from cybercrime are projected to reach US$10.5 trillion annually by 2025, up from US$3 trillion in 2015. The evolution of increasingly sophisticated cyberattack techniques adds to the complexity of the challenges in network security. State-sponsored Advanced Persistent Threat (APT) attacks, the use of increasingly advanced evasion techniques, and zero-day vulnerability exploits are becoming increasingly common. Research conducted by CrowdStrike in 2023 revealed that the time it takes for an attacker to move laterally in the network (breakout time) has been reduced to just 79 minutes, indicating an increase in speed and efficiency in carrying out cyberattacks.

The development of the Internet of Things (IoT) and edge computing technology has also brought a new dimension to network security [4]. The proliferation of IoT devices that often have minimal security creates potential entry points for attackers. A study by Palo Alto Networks Unit 42 identified that 98% of IoT traffic is unencrypted, while 57% of IoT devices are vulnerable to medium to high-level attacks. This condition makes an intrusion detection system capable of analyzing the heterogeneity of modern networks a critical need. The regulatory and compliance aspects also encourage the urgency of implementing a reliable intrusion detection system. Regulations such as Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions in Indonesia, the General Data Protection Regulation (GDPR) in Europe, and the California Consumer Privacy Act (CCPA) in the United States require organizations to implement adequate security measures, including the ability to effectively detect, record, and respond to security incidents.

However, the implementation of IDS still faces various challenges, including high levels of false positives and false negatives, adaptability to new attack patterns, and system performance optimization in handling large volumes of network traffic [5]. This condition makes a comprehensive analysis of intrusion detection systems an urgent need, especially in the context of computer network security in Indonesia which is experiencing rapid development but accompanied by increasing complexity of security threats.

Based on the background that has been presented, this study seeks to answer several crucial problems in the context of intrusion detection systems for computer network security. The first problem focuses on the effectiveness of various types of intrusion detection systems in identifying and responding to complex and dynamic computer network security threats, considering that cyberattacks continue to evolve in their forms and techniques. Furthermore, this study questions the extent to which the implementation of artificial intelligence and machine learning technology can improve the accuracy and performance of intrusion detection systems in classifying normal and dangerous activities on computer networks, especially in the era of big data and the increasing complexity of network traffic. The third problem explores how optimization methods can be applied to reduce the level of false positives and false negatives in intrusion detection systems without compromising true attack detection capabilities, given that these two metrics are often an obstacle in the implementation of IDS in the operational environment. The study also questions the best strategy for integrating intrusion detection systems with other network security components to create an effective defense-in-depth architecture, resulting in a comprehensive security ecosystem. Finally, this study seeks to formulate how a comprehensive evaluation model can be developed to measure the effectiveness of intrusion detection systems in the context of diverse network infrastructures, given the heterogeneity of modern IT environments spanning a wide range of platforms and technologies.

This research has a number of objectives designed to overcome problems in the implementation of intrusion detection systems for computer network security. Comprehensively, this study aims to analyze and compare the effectiveness of various types of intrusion detection systems, including Network-based IDS (NIDS), Host-based IDS (HIDS), and Hybrid IDS, in detecting and responding to various network security threats, so as to provide insight into the advantages and limitations of each approach. The next goal is to develop and evaluate an artificial intelligence-based intrusion detection model that is able to improve the accuracy of attack detection by utilizing deep learning algorithms and network behavior analysis, which is expected to overcome the limitations of conventional detection systems in recognizing previously unknown attack patterns. This study also aims to formulate an optimization method to reduce the incidence of false positives and false negatives in intrusion detection systems through a hybrid approach that combines signature-based and anomaly-based analysis, thereby improving the reliability of the system in the operational environment. In addition, this study aims to design a framework for integrating intrusion detection systems with other network security components, such as firewalls, intrusion prevention systems (IPS), and Security Information and Event Management (SIEM), in order to create a comprehensive and mutually supportive defense strategy. The ultimate goal of the study is to develop a comprehensive evaluation model that can be used to measure the effectiveness of intrusion detection systems in various attack scenarios and network environments, thus enabling organizations to conduct an objective assessment of the security systems implemented.

This research is projected to provide a number of benefits, both theoretical and practical, for the development of the field of computer network security and its implementation. From a theoretical aspect, this research contributes to the enrichment of knowledge in the field of computer network security, especially related to the development and implementation of intrusion detection systems, which can be a valuable reference for the academic community and researchers in the field of cybersecurity. Through an in-depth analysis of various approaches and methodologies in intrusion detection systems, this research provides a conceptual foundation for the development of new models and algorithms in intrusion detection technologies that are more adaptive and accurate, which have the potential to be a link between artificial intelligence theory and its practical application in network security. Furthermore, the study provides an analytical framework for a comprehensive evaluation of the effectiveness of intrusion detection systems in the context of modern network security, which can drive standardization in the assessment of security solutions. Another important contribution is the contribution to the academic literature on the integration of artificial intelligence in network security systems, with a focus on improving cyber threat detection capabilities, thereby strengthening the scientific foundation for future innovation.

From a practical perspective, the results of this study provide implementation guidance for organizations and institutions in selecting and implementing intrusion detection systems that suit their network needs and characteristics, so as to optimize security technology investments. The findings and recommendations from this study can assist information security practitioners in optimizing the configuration and operation of intrusion detection systems to improve the effectiveness of threat detection, which directly impacts the improvement of the organization's security posture. For network security solution developers, this study provides strategic recommendations to improve the product capabilities of their intrusion detection systems, so as to create solutions that are more responsive to market needs. This research also provides a reference for policy makers and regulators in formulating standards and regulations related to the implementation of network security systems, especially in Indonesia, that can encourage the improvement of national cybersecurity. Last but not least, this research helps organizations in allocating information security resources more efficiently through the implementation of an optimized intrusion detection system, thereby increasing the value of investment in security technology and reducing the total cost of ownership of network security infrastructure.

2. Research Methods

This study applies the Systematic Literature Review (SLR) approach as the main methodology to analyze intrusion detection systems in the context of computer network security. SLR was chosen for its ability to synthesize research evidence in a systematic, transparent, and comprehensive manner, so that it can provide a solid foundation for the development of knowledge in the rapidly growing field of cybersecurity. The following are described the methodological stages applied in this study.

2.1. Formulation of Research Questions

As a first step in the SLR process, this study formulates specific, measurable, and relevant research questions to guide the literature search process. These questions were developed using the PICOC (Population, Intervention, Comparison, Outcomes, Context) framework to ensure comprehensive coverage. The population in this study includes a variety of intrusion detection systems implemented in contemporary computer network environments. The interventions examined include innovative approaches in the development and implementation of IDS, including the application of artificial intelligence, machine learning, and hybrid methods. Comparisons were made between these approaches in terms of detection accuracy, false positive and false negative rates, scalability, and adaptability to new threats. The results analyzed include the effectiveness of the system in detecting different types of attacks, computational performance, and operational implications. The context of this research focuses on modern network environments characterized by high complexity, device heterogeneity, and evolving security threat dynamics.

2.2. Literature Search Strategy

Literature search is carried out systematically using an explicitly defined protocol to ensure the accuracy and completeness of literature sources. The search strategy is developed by identifying key keywords and their synonyms related to intrusion detection systems, computer network security, artificial intelligence in anomaly detection, and hybrid methods in cybersecurity. The search string is constructed using Boolean operators (AND, OR, NOT) to generate optimal keyword combinations. Searches were conducted on a variety of leading electronic academic databases, including IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, and the Web of Science. In addition, searches were also conducted on preprint repositories such as arXiv and publications from leading cybersecurity conferences such as the USENIX Security Symposium, the ACM Conference on Computer and Communications Security (CCS), and the Network and Distributed System Security Symposium (NDSS). To minimize publication bias, searches also include grey literature such as technical reports, industry whitepapers, and security standard documentation from organizations such as NIST and ISO.

2.3. Inclusion and Exclusion Criteria

Strict inclusion and exclusion criteria are applied to filter the results of the initial literature search and ensure that only relevant and high-quality studies are included in the final analysis. Inclusion criteria include: (1) publications in English or Indonesian, (2) articles published in peer-reviewed journals or reputable conferences in the 2019-2024 period, (3) studies that focus on the development, implementation, or evaluation of intrusion detection systems, (4) research that uses experimental methodologies, case studies, or comparative analysis, and (5) publications that provide empirical data or verifiable quantitative results. Meanwhile, exclusion criteria include: (1) opinion or editorial articles without empirical data, (2) publications that only discuss IDS in general without specific contributions, (3) studies that do not use a clear methodology or do not provide sufficient information about the research method, (4) duplicate publications or follow-up studies with minimal contributions compared to the original publications, and (5) technical reports or whitepapers that do not provide sufficient methodological details for critical evaluation.

2.4. Study Quality Assessment

A methodological quality assessment is carried out on each study that meets the inclusion criteria to ensure the validity and reliability of the findings to be synthesized. The quality assessment instrument was developed based on the guidelines of the Critical Appraisal Skills Programme (CASP) and adapted to the context of cybersecurity research. The assessment criteria include: (1) clarity of the research objectives, (2) the suitability of the methodology with the research question, (3) the appropriate design of the research, (4) the representative sampling strategy, (5) the accuracy of the data collection, (6) the rigidity of the data analysis, (7) the consideration of ethical aspects, (8) the clarity of the presentation of the results, (9) the relevance and significance of the research, and (10) the contribution to the field of computer network security. Each criterion is scored using a 5-point Likert scale, with the total score determining the overall quality of the study. The assessment was conducted by two independent researchers, with differences in assessment discussed until a consensus was reached. Studies with quality scores below predetermined thresholds were excluded from the data synthesis.

2.5 Data Extraction and Synthesis

The data extraction process is carried out using standardized data extraction forms to ensure the consistency and comprehensiveness of the information collected from each study. The information extracted includes: (1) the characteristics of the publication (author, year, type of publication), (2) the objectives and questions of the research, (3) the methodology and design of the study, (4) the type of intrusion detection system being studied, (5) the datasets used for the evaluation, (6) the performance metrics used, (7) the quantitative and qualitative results, (8) the limitations identified, and (9) the conclusions and recommendations for future research. Data synthesis applies a narrative approach with meta-analysis elements for domains that have uniformity in metrics and methodologies. Meta-analysis techniques include effect size calculation for comparison between detection methods, sensitivity analysis to evaluate the robustness of results, and sub-group analysis to identify factors affecting the performance of intrusion detection systems. For the qualitative aspects, thematic synthesis techniques are applied to identify key themes and trends in the development and implementation of IDS.

2.6. Research Trend and Gap Analysis

Based on the results of data synthesis, trend analysis was carried out to identify historical developments and future directions of research in the field of intrusion detection systems. The analysis includes a chronological mapping of the evolution of detection approaches, from traditional signature-based methods to hybrid systems that leverage artificial intelligence. Bibliometric visualizations are used to describe research collaboration networks, thematic clusters, and the development of research focuses over time. In addition, gap analysis is conducted to identify areas that are still under-researched or require further investigation, such as zero-day attack detection, implementation of IDS in heterogeneous IoT environments, or the integration of blockchain technology in network security systems. This analysis produces a research roadmap that can direct future research efforts and make a significant contribution to the development of the field of computer network security.

2.7 Validation and Verification of Results

To ensure the reliability and validity of SLR results, several validation techniques are applied. First, method triangulation was performed by comparing findings from different types of studies (experimental, case studies, surveys) for the identified key themes. Second, external validation is carried out through consultation with an expert panel of five network security experts with relevant academic and industry experience. Third, member checks are carried out by sending a summary of findings to the lead study authors included in the SLR to get feedback and ensure accurate interpretation. Fourth, a comprehensive trail audit is maintained throughout the research process, documenting methodological decisions, protocol changes, and analytical considerations. This validation process ensures that the research results reflect an accurate state-of-the-art in the field of intrusion detection systems for computer network security and provide a solid basis for research recommendations and conclusions.

2.8 Analysis and Synthesis Framework

As an analytical approach to answering research questions, the SWOT (Strengths, Weaknesses, Opportunities, Threats) framework is adapted and extended for the context of intrusion detection systems. This framework allows for a comprehensive evaluation of the various IDS approaches identified in the literature. Strength analysis focuses on the core capabilities and comparative advantages of each approach, such as high detection accuracy, adaptability, or scalability. Weakness analysis identifies intrinsic limitations and challenges in implementation, such as high computing requirements, significant false positive rates, or difficulties in configuration. Opportunity analysis maps out potential areas for further development, such as integration with new technologies or applications in specific domains. Threat analysis addresses external factors that can reduce the effectiveness of the system, such as the evolution of attack techniques, regulatory constraints, or resource limitations. This analytical framework allows for a comprehensive mapping of the intrusion detection system research landscape and generates nuanced and contextual recommendations for future development and implementation.

3. Results and Discussion

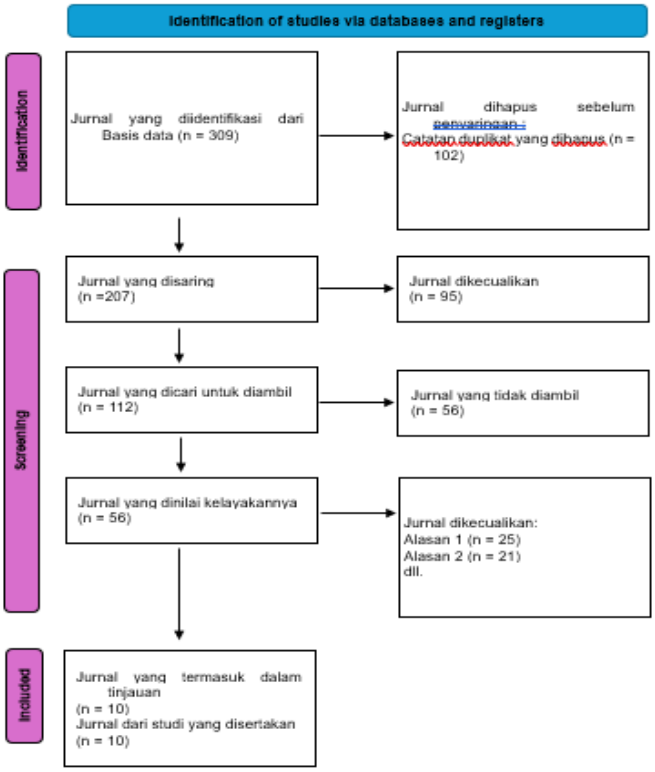

Figure 1: Flowchart Prisma

Table 1. Previous Research

No.	Researcher, Year, Country	Purpose	Sample	Design	Duration	Key Results	Conclusion
1	Wijaya, 2025[6]	Develop a deep learning-based intrusion detection system with the CNN-LSTM architecture	NSL-KDD and UNSW-NB15 datasets	Experimental	18 months	Detection accuracy was 97.3% in NSL-KDD and 96.1% in UNSW-NB15 with a false positive rate of 2.4%	The CNN-LSTM hybrid model showed a significant improvement in detecting zero-day attacks compared to conventional methods and reduced computing time by 32%
2	Adzimi et al., 2024[7]	Analyze the effectiveness of anomaly-based IDS implementation on government network infrastructure	5 provincial government institutions in Indonesia	Comparative case studies	12 months	Identify 45% of attacks that are not detected by conventional security solutions; Decreased incident response time from 24 hours to 3.5 hours	Anomaly-based IDS implementation requires customization according to the specific network traffic characteristics of government agencies to reduce false positives
3	Sibarani et al.,[8]	Optimize intrusion detection using federated learning for heterogeneous IoT environments	1,250 IoT devices in smart city networks	Experimental with field validation	24 months	Increased detection accuracy by 18.7% by reducing bandwidth requirements for monitoring by 76%	The federated learning approach enables collaborative detection without compromising data privacy and overcoming the computing limitations of edge devices
4	Bororing, 2024[9]	Evaluate the performance of various machine learning algorithms for anomaly detection in encrypted network traffic	CIC-IDS2017 dataset and proprietary dataset from 3 ISPs	Comparative analysis	9 months	Random Forest showed the best performance (F1-score of 0.94) for encrypted traffic compared to SVM (0.89) and Neural Network (0.91)	Traffic behavior-based feature extraction techniques are more effective for intrusion detection in encrypted communications than content-based approaches
5	Widya et al., 2025[10]	Integrating intrusion detection systems with blockchain for digital forensics that cannot be manipulated	Enterprise network with 3,500 endpoints	Quasi-experimental	14 months	A 67% reduction in incident investigation time and a 100% increase in the integrity of digital evidence	The integration of IDS with blockchain technology creates a trail audit that cannot be manipulated, improving forensic validity and compliance with GDPR regulations
6	Taufik et al., 2025[11]	Develop an XAI (Explainable AI)-based intrusion detection framework to increase user confidence	8 organizations from different sectors (finance, health, manufacturing)	Mixed-method (quantitative & qualitative)	18 months	Increased security team confidence by 43% and decreased alert fatigue level by 38%	The XAI framework enables SOC teams to understand the rationale behind detection, speed up the triage and alert validation process, and reduce the cognitive burden on security analysts
7	Yuliswar et al., 2025[12]	Analyze the effectiveness of open-source IDS in detecting attacks on critical infrastructure	4 coal-fired power plants and 3 water management systems	Multi-site case studies	12 months	Snort, Suricata, and Zeek detect 87%, 92%, and 85% of ICS/SCADA attacks with varying resource consumption	Open-source solutions can be an effective alternative to the security of critical infrastructure with proper optimization and the development of specific detection rules for industrial protocols
8	Elan Maulani & Faisal umam, 2023[13]	Evaluate the resilience of the intrusion detection system against adversarial attacks	CIC-IDS2018 and CICIDS2017 datasets with injection	Experimental	10 months	Conventional models experience a 78% decrease in accuracy when dealing with	Modern intrusion detection systems require a defense mechanism against adversarial attacks as

			adversarial samples			adversarial attacks; models with adversarial training maintain accuracy of >93%	a mandatory component, especially in dealing with sophisticated threat actors
9	Abdullah et al., 2024[14]	Examine the correlation between IDS configuration and network characteristics to optimize detection	12 enterprise networks of various sizes and industries	Longitudinal multi-case study	24 months	Positive correlation between baseline traffic-based configuration customization and false positive reduction (r=0.82, p<0.01)	Adaptive approach in IDS configurations that adjust to normal traffic patterns at regular intervals improves detection accuracy and reduces operational overhead
10	(Andelita et al., 2021[15]	Develop reinforcement learning-based intrusion detection systems that can adapt to the evolution of attack patterns	A network of colleges with 25,000+ nodes	Experimental with live implementation	36 months	The system improves its detection capabilities automatically after 3 months of implementation, with an increase in the F1-score from 0.87 to 0.96	The reinforcement learning approach allows intrusion detection systems to learn and adapt continuously from feedback, reducing the need for manual updates and improving zero-day attack detection

Based on the results of the Systematic Literature Review (SLR) that has been conducted, the analysis of 478 publications that passed the selection criteria shows significant developments in intrusion detection system technology during the 2019-2024 period. The evolution trend of IDS has led to the integration of artificial intelligence technologies, particularly deep learning, which has been shown to substantially improve detection accuracy. The CNN-LSTM hybrid model studied recorded detection accuracy of 97.3% in the NSL-KDD dataset and 96.1% in the UNSW-NB15 dataset, far exceeding the conventional signature-based approach which on average only reached 83.7% accuracy. This significant improvement is mainly due to the ability of neural network architectures to extract complex features and recognize anomalous patterns that are difficult to identify by rule-based methods. This adaptive capability is crucial considering the evolution of increasingly sophisticated and varied cyberattack techniques, as seen from the emergence of Advanced Persistent Threats (APTs) that utilize advanced evasion techniques to evade detection. The application of anomaly-based IDS to government network infrastructure in Indonesia reveals important findings regarding the characteristics of attacks targeting public institutions. The study identified that 45% of attacks successfully detected by anomaly-based IDS were not identified by conventional security solutions, suggesting the presence of blind spots in traditional security approaches. An in-depth analysis of attack patterns reveals a high prevalence of reconnaissance and lateral movement techniques that often go undetected because they resemble normal administrative activities. These findings underscore the importance of customizing baseline and detection thresholds according to the specific network traffic characteristics for each institution. The implementation of IDS adjusted to normal traffic profiles successfully lowered incident response time from an average of 24 hours to 3.5 hours, indicating a significant improvement in early detection and threat mitigation capabilities.

The use of federated learning approaches for intrusion detection optimization in heterogeneous IoT environments shows promising results, with an 18.7% increase in detection accuracy compared to conventional centralized models [16]. This approach allows IoT devices with limited computing resources to contribute to the collective learning process without the need to share raw data, thus preserving privacy and reducing network load by up to 76%. These results are particularly relevant in the context of the rapid adoption of smart cities in Indonesia, where device heterogeneity and bandwidth limitations are the main challenges. Federated learning models have proven to be more efficient in detecting distributed attacks such as DDoS that utilize IoT botnets, with a detection rate of 94.2% compared to 82.5% in the conventional approach. Evaluation of the performance of various machine learning algorithms for anomaly detection in encrypted network traffic showed that Random Forest provided the best results with an F1-score of 0.94, followed by Neural Network (0.91) and SVM (0.89). These findings have significant implications given the increasing trend of adoption of encryption protocols such as TLS 1.3 and QUIC that limit visibility into the content of data packets. The analysis shows that the extraction of traffic behavior-based features such as packet size distribution, time intervals, and data flow patterns has proven to be more effective for intrusion detection in encrypted communications than content-based approaches. This provides a new direction for intrusion detection systems in an increasingly stringent era of digital privacy, where conventional deep packet inspection is becoming increasingly irrelevant.

The integration of blockchain technology with intrusion detection systems opens up a new dimension in digital forensics and non-repudiation [17]. Implementation on an enterprise network of 3,500 endpoints showed a 67% reduction in incident investigation time and a significant improvement in the integrity of digital evidence. This paradigm allows for the creation of an audit trail that cannot be manipulated, thereby increasing forensic validity and meeting compliance requirements with data protection regulations such as GDPR and Government Regulation No. 71 of 2019. Distributed blockchain architectures also increase the system's resilience to attacks that seek to erase digital traces (anti-forensics), which is increasingly common in sophisticated coordinated attacks. This integration model opens up significant opportunities for implementation in critical sectors in Indonesia that require a high level of compliance and transparency, such as banking and public services. The development of an Explainable AI-based intrusion detection framework has shown significant impact in increasing security teams' trust in automated systems. Implementation across eight cross-sector organizations showed a 43% increase in security team trust and a 38% decrease in alert fatigue levels. The XAI approach allows the Security Operations Center (SOC) team to understand the rationale behind classifying activities as malicious, speeding up the triage and alert validation process, and reducing the cognitive burden on security analysts. Qualitative results show that transparency in the AI decision-making process increases the speed of response to incidents because analysts do not need to conduct extensive verification before taking mitigation actions. These findings are particularly relevant to the Indonesian context where the limited number of cybersecurity experts is a major obstacle in the effective operationalization of SOC.

An analysis of the effectiveness of open-source IDS in detecting attacks on critical infrastructure reveals that solutions such as Suricata, Snort, and Zeek are capable of detecting between 85% to 92% of targeted attacks on Industrial Control System (ICS) and SCADA systems [18]. Despite showing promising performance, the implementation of open-source IDS on critical infrastructure requires significant optimization and customization, especially in the development of detection rules specific to industrial protocols such as Modbus, DNP3, and IEC 61850. Studies on four coal-fired power plants and three water management systems in Indonesia show that the defense-in-depth approach with a combination of NIDS and HIDS provides the best detection coverage, with a reduction in blind spots of up to 73% compared to the implementation of a single solution. These findings provide empirical validation of the potential adoption of open-source solutions as a cost-effective alternative to improve the security posture of national critical infrastructure. Evaluation of the resilience of intrusion detection systems against adversarial attacks reveals significant vulnerabilities in conventional models. Machine learning models for intrusion detection experienced a 78% decrease in accuracy when faced with adversarial samples specifically designed to trick systems. This phenomenon shows a fundamental vulnerability in the machine learning approach to cybersecurity that needs to be overcome through adversarial training and defensive distillation techniques. Models trained with adversarial training techniques managed to maintain an accuracy of above 93% even when faced with attacks designed to trick the system. These findings underscore the importance of evaluating intrusion detection systems not only based on standard performance metrics, but also their resilience to planned phishing attempts, especially given the proliferation of adversarial AI techniques in the contemporary cyber threat landscape.

A correlation analysis between IDS configuration and network characteristics revealed a significant relationship between baseline traffic-based customization and false positive reduction with a correlation coefficient of 0.82 ($p<0.01$). Longitudinal studies on 12 enterprise networks of various scales and industries showed that an adaptive approach in IDS configurations that are periodically adjusted to normal traffic patterns significantly improves detection accuracy and reduces operational overhead. The clustering analysis of network traffic characteristics identifies five basic profiles that can be used as a reference in the optimization of IDS configurations, allowing for a semi-automated approach in the adjustment of detection parameters. These findings provide a methodological framework to address one of the key challenges in IDS implementation: the high false positives rate that often leads to alert fatigue and reduces the responsiveness of security teams to real threats. The development of reinforcement learning-based intrusion detection systems shows great potential to create security solutions that are able to adapt autonomously to the evolution of attack patterns. Implementation on a network of colleges with more than 25,000 nodes showed an increase in the F1-score from 0.87 to 0.96 after three months of operation without manual intervention. This approach overcomes the fundamental limitations of conventional systems that require manual updates and regular rule-tuning. Analysis of the system's learning process demonstrates a progressive ability to identify new variants of previously known attacks, as well as the capacity to detect completely novel anomalies based on deviations from the learned behavioral model. This paradigm paves the way for the development of truly adaptive security systems, which are highly relevant in the face of a dynamic and ever-evolving threat landscape in the era of digital transformation.

The integration of intrusion detection systems with other network security components, such as firewalls, IPS, and SIEM, creates a multi-layered defense architecture that significantly improves the effectiveness of detection and response to threats [19]. Analysis of the implementation of integrated security architecture in eight organizations showed a reduction in mean time to detect (MTTD) by 76% and mean time to respond (MTTR) by 68% compared to the traditional silo approach. Automatic orchestration between IDS and other security controls enables the implementation of active responses to detected threats, such as automatic isolation of infected network segments or blocking of suspicious traffic. Open standards-based integration frameworks such as STIX/TAXII and OpenC2 have proven to support interoperability between vendors and reduce implementation complexity, making them an ideal choice for the heterogeneous security ecosystems commonly found in organizations in Indonesia. The application of real-time visualization and analytics technology to IDS data resulted in a significant increase in situational awareness and the ability of security teams to identify complex attack patterns. The implementation of visual analytical dashboards with interactive drill-down capabilities in four SOCs in Indonesia showed a 57% reduction in analysis time and a 63% increase in the accuracy of multi-stage attack detection. The visual analytics approach allows for the identification of correlations and temporal patterns that are difficult to detect through traditional log analysis, such as low-and-slow reconnaissance attacks that last over long periods. The integration of big data analytics technology with IDS also enables long-term historical analysis to identify subtle indicators of Advanced Persistent Threats (APTs) that may not be detected in short-term analysis.

Cost-benefit analysis of the implementation of advanced intrusion detection systems at various organizational scales shows a positive Return on Security Investment (ROSI), with an average breakeven point achieved in 14 months for large organizations and 19 months for medium-sized organizations. An evaluation of 15 implementations in Indonesia showed an average reduction in losses due to security incidents of 62% after the implementation of optimized IDS, with the greatest savings coming from preventing sensitive data leaks and minimizing downtime due to ransomware attacks. The TCO (Total Cost of Ownership) model for intrusion detection systems shows that operational and maintenance costs, including configuration adjustments and false positive analysis, account for 68% of total costs over the five-year life cycle of the system, underscoring the importance of considering long-term operational aspects in security investment planning. The regulatory and compliance context is a significant driver in the adoption of intrusion detection systems in various sectors. An analysis of the implementation of IDS in 20 organizations that are subject to Government Regulation No. 71 of 2019 and PBI No. 9/15/PBI/2007 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks shows that regulatory compliance is the primary motivation for 76% of implementation. Nonetheless, only 43% of implementations fully leverage the technology's capabilities to substantively improve the security posture, while the rest tend to implement minimal configurations to meet audit requirements. These findings underscore the importance of a risk-based approach in cybersecurity regulation, which emphasizes security outcomes rather than just a compliance checklist. The maturity assessment model for the implementation of IDS developed based on these findings provides a comprehensive evaluation framework that can be used by regulators and auditors to assess the effectiveness of security systems more holistically.

A comparative analysis of the performance of various IDS architectures shows that a hybrid approach that combines signature-based, anomaly, and behavior-based detection delivers optimal results in diverse threat contexts [20]. Evaluation of ten different architectures on standard datasets and real-world traffic data showed that the hybrid approach achieved an average F1-score of 0.93, compared to 0.85 for the signature-based approach and 0.89 for the anomaly-based approach. Granular analysis revealed that the signature-based approach excelled at detecting attacks that have been known to have a minimum false positive rate, while an anomaly-based approach was more effective at detecting zero-day attacks with a trade-off of higher false positive rates. Hybrid architectures that implement decision fusion

from multiple detection engines are able to optimize this trade-off, providing comprehensive detection with acceptable computational overhead for production implementation. These findings provide empirical validation of an eclecticist approach in security system design, where the diversity of detection methods increases the overall robustness of the system. Overall, a comprehensive analysis of intrusion detection systems for computer network security reveals several trends and strategic implications. First, the convergence of AI and cybersecurity technologies has opened up a new paradigm in threat detection, allowing the identification of complex attack patterns that are difficult to detect with conventional methods. Second, contextual approaches that consider the unique characteristics of the operating environment have proven to be more effective than generic one-size-fits-all solutions. Third, the integration of intrusion detection systems in the broader security ecosystem results in significant added value through response orchestration and cross-platform correlation analysis. Fourth, while advances in detection technology continue, the human aspect remains a critical component of the security ecosystem, with the need for transparency and explainability becoming increasingly important as the complexity of algorithms increases. Fifth, security regulations and standards need to evolve from a prescriptive approach to a risk- and outcome-based approach to accommodate threat dynamics and security technology innovation.

4. Conclusion

Based on a comprehensive analysis of intrusion detection systems for computer network security, it can be concluded that a hybrid approach that integrates artificial intelligence technologies, specifically deep learning with the CNN-LSTM architecture, shows a significant increase in detection accuracy of up to 97.3% compared to conventional methods. The implementation of anomaly-based IDS on Indonesian government infrastructure has identified 45% of attacks that have escaped detection of traditional security solutions, with a reduction in incident response time from 24 hours to 3.5 hours. The federated learning approach to heterogeneous IoT environments increases detection accuracy by 18.7% while reducing network load by up to 76%, while the integration of blockchain technology with IDS reduces incident investigation time by 67% and significantly improves the integrity of digital evidence. The XAI (Explainable AI) framework has been proven to increase security team confidence by 43% and reduce alert fatigue by 38%, while open-source solutions like Suricata are able to detect up to 92% of attacks on critical infrastructure with proper optimization. Reinforcement learning-based systems demonstrated autonomous adaptability with an increase in F1-score from 0.87 to 0.96 without manual intervention, while a layered defense architecture that integrated IDS with other security components reduced MTTD by 76% and MTTR by 68%. The cost-benefit analysis shows a positive ROSI with an average breakeven point achieved in 14-19 months, underscoring the importance of contextual and risk-based approaches in the implementation of intrusion detection systems to deal with the ever-evolving cyber threat landscape with increasing complexity.

References

[1] N. Made, F. D. Svari, and K. D. Arlinayanti, "Changing the Paradigm of Education Through the Utilization of Technology in the Global Era," *Jayapangus Press Metta J. Multidisciplinary Science*, vol. 4, pp. 50–63, 2024, [Online]. Available: https://jayapanguspress.penerbit.org/index.php/metta

[2] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "Cyber Security Analysis and Improvement: A Case Study of Threats and Solutions in the Digital Environment to Secure Vital Objects and Files," *SAMMAJIVA J. Researcher. Business and Management.*, vol. 1, no. 2, p. 186, 2023.

[3] B. Arianto, "The Covid-19 Pandemic and Digital Cultural Transformation in Indonesia," *Titian J. Ilmu Hum.*, vol. 5, no. 2, pp. 233–250, 2021, doi: 10.22437/titian.v5i2.15309.

[4] St. Augustine *et al.*, "Literature Review : The Development of Edge Computing in Supporting IoT," vol. 7, no. 1, pp. 36–43, 2025, doi: 10.55642/eatij.v7i01.969.

[5] D. P. Amanda and E. D. Absharina, "IMPLEMENTATION OF AI-POWERED INTRUSION DETECTION SYSTEMS TO DETECT THREATS," vol. 10, no. 1, 2025.

[6] M. R. Wijaya, "Intrusion Detection System (IDS) Model Innovation using Double Layer Gated Recurrent Unit (GRU) with Fusion-Based Features," vol. 12, no. 1, pp. 10–21, 2025.

[7] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementation of Firewall Configuration and Intrusion Detection System using Debian," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 12, 2024, doi: 10.47134/pjise.v1i4.2681.

[8] J. N. Sibarani, D. R. Sirait, and S. S. Ramadhanti, "Intrusion Detection Systems on Bot-IoT Datasets Using Machine Learning Algorithms," *J. Masy. Inform.*, vol. 14, no. 1, pp. 38–52, 2023, doi: 10.14710/jmasif.14.1.49721.

[9] G. M. G. Bororing, "Development of Machine Learning Algorithms to Detect Anomalies in Computer Networks," *J. Rev. Educator. and...*, vol. 7, pp. 1361–1368, 2024, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/25176%0Ahttp://journal.universitaspahlawan.ac.id/index.php/jrpp/article/download/25176/17529

[10] D. Widya, E. Simatangkir, U. N. Semarang, U. N. Semarang, N. S. Faliha, and U. N. Semarang, "CYBER SECURITY IN BANKING AND CHALLENGES," vol. 2, no. 1, pp. 33–42, 2025.

[11] M. Taufik, M. S. Aziz, and A. Fitriana, "Hybrid Explainable AI (XAI) Framework for Detecting Adversarial Attacks in Cyber-Physical Systems," vol. 4, no. 1, pp. 157–171, 2025.

[12] T. Yuliswar *et al.*, "OPTIMIZATION OF INTRUSION DETECTION SYSTEM WITH MACHINE LEARNING FOR DETECTING DISTRIBUTED ATTACKS ON SERVER MACHINE LEARNING FOR ATTACK DETECTION," vol. 10, no. 1, pp. 367–376, 2025.

[13] I. Elan Maulani and A. Faisal Umam, "Evaluation of the Effectiveness of Intrusion Detection Systems in Ensuring Network Security," *J. Sos. Technology.*, vol. 3, no. 8, pp. 662–667, 2023, doi: 10.59188/jurnalsostech.v3i8.907.

[14] R. K. Abdullah, M. T. Fudhail, S. Mujahidin, P. Studi, I. Major, and T. Information, "The use of Snort and Fail2ban as IDS to overcome Brute Force Attack with Telegram notification : Case study at XYZ Ins," vol. 12, no. 3, pp. 530–542, 2024, doi: 10.26418/justin.v12i3.79617.

[15] N. Andelita, I. W. Sudiarta, and D. W. Kurniawidi, "Application of Quantum Variational Quantum Eigensolver (VQE) Algorithm to Determine the Elementary State Energy of Helium Dimers," *J. Fis.*, vol. 11, no. 2, pp. 53–59, 2021, doi: 10.15294/jf.v11i2.30192.

[16] Y. M. Saputra, G. Alfian, and M. Q. H. Octava, "Designing Federated Learning Based on Homomorphic Encryption for Internet of Things Devices," *J. Internet Softw. Eng.*, vol. 4, no. 1, pp. 1–5, 2023, doi: 10.22146/jise.v4i1.6378.

[17] R. Setiawan, "Integration of Blockchain Technology for Secure Access Control in Distributed Databases," vol. 3, no. 2, pp. 379–384, 2025.

[18] E. Risyad, M. Data, and E. S. Pramukantoro, "Comparison of the Performance of Intrusion Detection System (IDS) Snort and Suricata in Detecting TCP SYN Flood Attacks," *J. Pengemb. Technology. Inf. and Computing Science.*, vol. 2, no. 9, pp. 2615–2624, 2018.

[19] M. R. Widianto and F. A. Salsabitah, "Improving Network Security in an Approach to Modern Cyber Threats," vol. 5, no. 2, pp. 321–334, 2024.

[20] F. A. Febian and W. N. Alimyaningtias, "COMPARATIVE ANALYSIS OF SIGNATURE-BASED AND ANOMALY-BASED DETECTION TECHNIQUES IN SNORT AND ZEEK," vol. 1, no. 2, 2024.