International Journal of Computer Technology and Science
Volume. 1 No. 2 April 2024
e-ISSN :3048-1961, And p-ISSN :3048-1899, Page. 42-54
DOI: https://doi.org/10.62951/ijcts.v1i2.63
Available online at: https://international.arteii.or.id/index.php/IJCTS

Automated Detection Of Network Intrusions Using Machine Learning in Real-Time Systems

Aulia Novi[1*], Ryan Satria[2]
[1-2]Hasanuddin University (UNHAS), Indonesia

Abstract. *The rapid growth of digital technologies has significantly increased the complexity and frequency of cyber threats, making network security a critical concern in modern information systems. Traditional security approaches, such as rule-based and signature-based systems, are often limited in detecting sophisticated and unknown attacks. Therefore, this study proposes an Anomaly-Based Intrusion Detection System (AbIDS) utilizing machine learning and deep learning techniques to enhance detection capabilities. The research adopts a Design Science Research approach, involving stages of problem identification, data collection, preprocessing, model development, system implementation, and evaluation. Several models, including Decision Tree (DT), Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM), are implemented and compared. The results indicate that deep learning models, particularly LSTM and CNN, outperform traditional machine learning methods in terms of accuracy, precision, recall, and F1-score, while maintaining a lower false positive rate. Additionally, the integration of incremental learning enables the system to adapt to new attack patterns without requiring complete retraining, improving scalability and real-time performance. Despite the promising results, challenges such as computational complexity and false positives remain. Overall, the proposed IDS model demonstrates strong potential as an effective and adaptive solution for enhancing network security in dynamic environments.*

Keywords: *Anomaly Detection; Deep Learning; Intrusion Detection System; Machine Learning; Network Security.*

1. INTRODUCTION

In the rapidly evolving digital era, network security has become a critical aspect of maintaining the integrity and reliability of information systems. The widespread adoption of technologies such as the Internet, cloud computing, and big data has accelerated digital transformation across various sectors. However, this advancement has also significantly increased the exposure to cybersecurity threats, both in terms of frequency and complexity, requiring more intelligent and adaptive security mechanisms [1]. Along with technological advancements, cyberattacks have become more sophisticated, including polymorphic malware, distributed denial-of-service (DDoS) attacks, and zero-day exploits. These types of attacks are increasingly difficult to detect using traditional security approaches. Conventional systems, such as firewalls and rule-based detection mechanisms, rely heavily on predefined signatures and rules, which limits their ability to identify novel or evolving threats. Furthermore, these approaches are generally reactive in nature, making them less effective in proactively mitigating emerging cyber threats [2], [3].

To address these limitations, there is a growing need for more advanced and adaptive intrusion detection mechanisms. One promising solution is the implementation of Intrusion Detection Systems (IDS) based on machine learning techniques. Machine learning enables systems to automatically learn patterns from network traffic data and detect anomalies that may

indicate malicious activities. This approach improves detection accuracy and reduces false positive rates compared to traditional methods [4], [5]. Moreover, machine learning-based IDS can identify previously unknown attacks through anomaly detection techniques, providing a significant advantage in dynamic and evolving network environments. Various machine learning algorithms, such as decision trees, support vector machines, and neural networks, have demonstrated strong performance in enhancing intrusion detection capabilities [2], [6].

Despite its advantages, the implementation of machine learning in intrusion detection systems presents several challenges, particularly in achieving real-time detection. These challenges include the need for high-quality training data, scalability to handle large volumes of network traffic, and robustness against adversarial attacks. Additionally, processing speed becomes a critical factor to ensure timely responses to potential threats [1], [7].

Given the increasing complexity of cyber threats and the limitations of traditional security systems, the development of a machine learning-based intrusion detection system that is accurate, adaptive, and capable of real-time operation has become an urgent necessity. Therefore, this study focuses on designing and evaluating a machine learning-based intrusion detection model to enhance network security in modern digital environments.

2. LITERATURE REVIEW

Basic Concepts of Network Security

Network security is a fundamental aspect of modern information systems, focusing on protecting data and network infrastructure from unauthorized access, misuse, and cyber threats. It involves the implementation of policies, technologies, and management practices to ensure data confidentiality, integrity, and availability. According to Ali et al., (2024) , network security encompasses both hardware and software mechanisms, including firewalls, intrusion detection systems (IDS), and cryptographic techniques, to safeguard data during transmission. Similarly, Nithya et al., (2019) emphasize the role of cryptographic algorithms in securing communication channels and preventing data breaches.

In practice, network security management requires continuous monitoring and control of network traffic by administrators in both public and private network environments. Security mechanisms are designed not only to prevent attacks but also to detect and respond to suspicious activities in real time. Abdulkadhim & Hasan, (2021) highlight that integrating multiple security layers can significantly enhance network performance and resilience against cyber threats.

Types of Network Attacks

With the rapid advancement of digital technologies, various types of network attacks have emerged, posing significant challenges to cybersecurity. One of the most common types is Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, which aim to overwhelm a server or network with excessive traffic, rendering services unavailable. These attacks are often executed using botnets, which are networks of compromised devices controlled by attackers [11].

Another major category of threats is malware, which includes viruses, worms, ransomware, and trojans. These malicious programs are designed to disrupt system operations, steal sensitive data, or gain unauthorized access to networks. According to Alshamsi et al., (2024), malware attacks have become increasingly sophisticated, especially in smart environments such as smart homes and Internet of Things (IoT) ecosystems.

In addition to technical attacks, social engineering remains a significant cybersecurity threat. This type of attack manipulates individuals into revealing confidential information or granting unauthorized access, often through deception or psychological tactics. As noted by Aslan et al., (2023), social engineering exploits human vulnerabilities rather than technical weaknesses, making it particularly challenging to mitigate. Furthermore, the proliferation of IoT devices has introduced new security challenges. IoT networks are often targeted by attacks such as phishing, DoS, and zero-day exploits due to their limited security capabilities and heterogeneous nature. These vulnerabilities make IoT systems attractive targets for cybercriminals [12].

Prevention and Security Measures

To mitigate the risks associated with network attacks, various preventive measures and security strategies have been developed. One of the primary defenses is the use of firewalls and intrusion detection systems (IDS), which monitor network traffic and identify suspicious activities. Modern IDS solutions, such as those based on Suricata, are capable of detecting and isolating threats in real time, thereby enhancing network security [13].

Cryptographic techniques also play a crucial role in securing data transmission. Encryption algorithms ensure that sensitive information remains confidential and protected from unauthorized access. As highlighted by [9], cryptographic models are essential for maintaining data integrity and confidentiality in network communications.

Another important aspect of network security is user awareness and training. Human error is often a major factor in successful cyberattacks, particularly in cases involving phishing and social engineering. Educating users about cybersecurity best practices can significantly

reduce the likelihood of such attacks [11]. In addition, implementing a multi-layered security approach that combines technical solutions with organizational policies is considered an effective strategy. This approach enhances the overall security posture by addressing both technological and human-related vulnerabilities [10].

Intrusion Detection System (IDS): Overview, Types, and Analysis

Definition of Intrusion Detection System

An Intrusion Detection System (IDS) is a hardware or software solution designed to monitor network or system activities in order to detect malicious behavior or violations of security policies. The primary objective of an IDS is to identify, track, and report suspicious activities so that preventive actions can be taken to minimize the impact of potential cyberattacks. IDS can be deployed in different forms, including Network-based Intrusion Detection Systems (NIDS), which monitor network traffic, and Host-based Intrusion Detection Systems (HIDS), which focus on activities within individual devices or hosts [14].

In modern cybersecurity frameworks, IDS plays a critical role as a defensive mechanism that complements other security tools such as firewalls and encryption systems. With the increasing complexity of cyber threats, IDS technologies have evolved to incorporate advanced data processing and machine learning techniques to improve detection capabilities [15].

Types of IDS: Signature-Based vs Anomaly-Based

Intrusion Detection Systems can generally be classified into two main categories: signature-based IDS (SbIDS) and anomaly-based IDS (AbIDS). Signature-based IDS detects attacks by comparing observed network traffic against a database of known attack signatures. This method is highly effective in identifying previously known threats with high accuracy. However, its major limitation lies in its inability to detect new or unknown attacks, including zero-day exploits, as it relies solely on predefined patterns [16].

On the other hand, anomaly-based IDS utilizes machine learning and statistical techniques to establish a baseline of normal system behavior. Any deviation from this baseline is flagged as a potential intrusion. This approach is particularly suitable for detecting novel and evolving threats in dynamic network environments. Research by Laghrissi et al., (2021) demonstrates that advanced models such as Long Short-Term Memory (LSTM) can effectively capture temporal patterns in network traffic, improving anomaly detection performance.

Despite its advantages, anomaly-based IDS also presents several challenges. One of the primary issues is the high rate of false positives, which can overwhelm security analysts and reduce system reliability. Additionally, anomaly-based systems typically require substantial

computational resources and large volumes of training data to achieve optimal performance [15], [16].

Strengths and Limitations of IDS

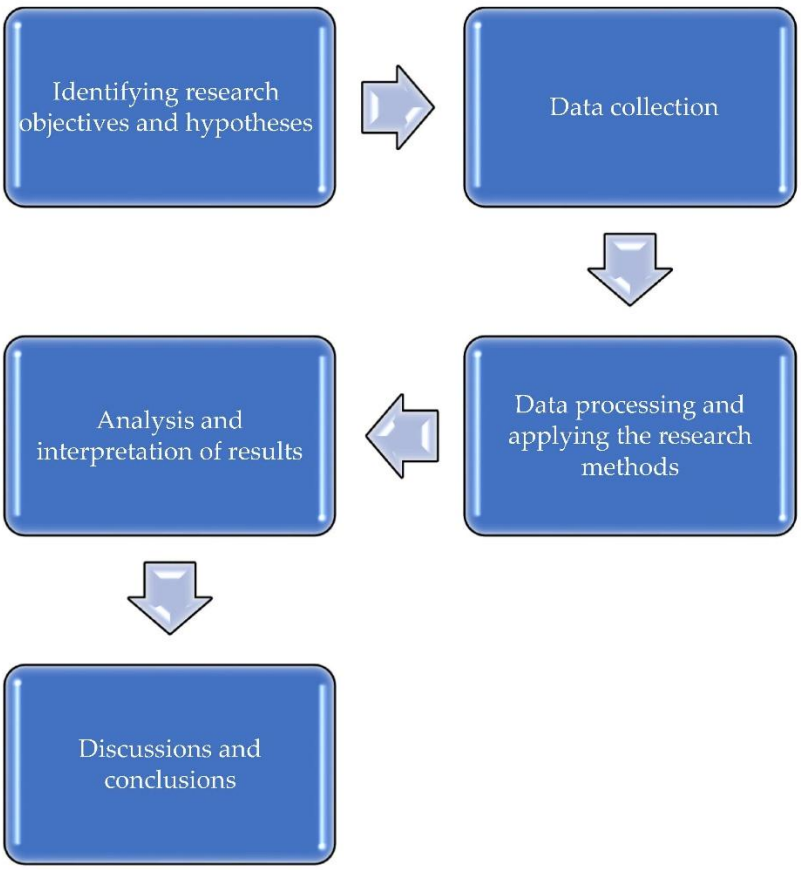
Overall, IDS provides significant benefits in enhancing network security. One of its key strengths is its ability to be integrated with machine learning algorithms, enabling more adaptive and intelligent threat detection. Techniques such as Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN) have been widely used to improve detection accuracy and classification performance in IDS applications [18], [19]. Furthermore, feature selection techniques play an important role in improving IDS efficiency by reducing data dimensionality and enhancing classification accuracy. Heryanto et al., (2022) highlight that correlation-based feature selection methods can significantly improve the detection performance while reducing computational complexity.

However, IDS also has several limitations. One of the major challenges is the occurrence of false positives and false negatives, which can affect the reliability of the system. False positives may lead to unnecessary alerts, while false negatives can result in undetected attacks. Additionally, the high computational cost, especially in anomaly-based systems, can limit scalability and real-time implementation [16]. Recent studies have also explored incremental learning approaches to improve IDS adaptability in dynamic environments. Kuswara et al., (2023) demonstrate that incremental learning methods enable IDS to continuously update its knowledge without retraining from scratch, making it more suitable for real-time applications.

Summary of IDS Characteristics

In summary, IDS is an essential component of modern cybersecurity infrastructure. The choice between signature-based and anomaly-based approaches depends on the specific requirements of the organization, including the need for accuracy, adaptability, and computational efficiency. While signature-based IDS offers high precision for known threats, anomaly-based IDS provides better capability in detecting unknown attacks. Therefore, hybrid approaches that combine both techniques are increasingly being adopted to overcome the limitations of each method and enhance overall system performance.

3. RESEARCH METHOD



Picture 1. Proposed Research Methodology Framework

Research Approach

This study adopts a Design Science Research (DSR) approach to develop and evaluate an effective Intrusion Detection System (IDS) based on machine learning techniques. The DSR approach is chosen because it focuses on designing, implementing, and evaluating artifacts that solve real-world problems, particularly in cybersecurity systems. The proposed artifact in this research is a machine learning-based IDS model capable of detecting network intrusions in real time.

Data Collection

The dataset used in this study is obtained from publicly available network intrusion datasets, which contain both normal and malicious traffic. These datasets typically include various types of attacks such as Denial-of-Service (DoS), probing, user-to-root (U2R), and remote-to-local (R2L) attacks.

The data consists of multiple features representing network traffic characteristics, including protocol type, duration, number of bytes transferred, and connection status. These

features are essential for training machine learning models to distinguish between normal and abnormal behaviors.

Model Development

This study develops an Anomaly-Based Intrusion Detection System (AbIDS) using various machine learning algorithms. Several models are implemented and compared, including Decision Tree (DT), Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). Among these, CNN is utilized for pattern recognition in network traffic data, while LSTM is employed to capture temporal dependencies in sequential traffic patterns, enabling more effective detection of complex and evolving attacks. Additionally, an incremental learning approach is incorporated to allow the system to adapt to new patterns without requiring retraining from scratch, thereby improving scalability and supporting real-time intrusion detection performance.

System Architecture

The proposed IDS system consists of several integrated components designed to support efficient intrusion detection. The process begins with the data input layer, which receives network traffic data in both real-time and batch modes. This data is then processed in the preprocessing module, where it is cleaned and transformed into a suitable format for analysis. Next, the feature selection module identifies the most relevant features to reduce dimensionality and improve system performance. The processed data is then analyzed by the detection engine, which applies machine learning models to classify network traffic as normal or malicious. Finally, the alert system generates notifications whenever potential intrusions are detected. This architecture is designed to support both offline training and real-time detection scenarios, ensuring flexibility and adaptability in various network environments.

Model Evaluation

The performance of the proposed IDS model is evaluated using several standard metrics to ensure comprehensive assessment. Accuracy is used to measure the overall correctness of the model in classifying network traffic. Precision indicates the proportion of correctly detected attacks among all predicted attack instances, while recall, also known as the detection rate, measures the model's ability to identify actual attack occurrences. The F1-score is employed as the harmonic mean of precision and recall to provide a balanced evaluation of the model's performance. Additionally, the false positive rate (FPR) is used to assess the extent to which normal traffic is incorrectly classified as malicious. These evaluation metrics are essential for comparing the performance of different machine learning models and determining the most effective approach for intrusion detection.

Experimental Setup

The experiments are conducted using a simulation environment that mimics real-world network conditions. The dataset is divided into training and testing sets, typically using an 80:20 ratio.

Machine learning models are trained using the training dataset and evaluated on the testing dataset. Hyperparameter tuning is performed to optimize model performance. The system is also tested under different attack scenarios to evaluate its robustness and adaptability.

System Evaluation

The proposed system is evaluated based on its ability to effectively detect both known and unknown attacks, reduce false positive rates, operate efficiently in real-time environments, and adapt to dynamic network conditions. These evaluation criteria are essential to ensure that the system can handle modern and evolving cybersecurity threats. Furthermore, the performance results of the proposed system are compared with traditional signature-based IDS approaches to demonstrate the advantages of the machine learning-based model in terms of accuracy, adaptability, and overall detection capability.

Research Flow

The overall research process begins with problem identification and a comprehensive literature review to establish the research foundation and identify gaps in existing studies. This is followed by data collection and preprocessing to ensure the dataset is clean, structured, and suitable for analysis. Subsequently, the model development phase is carried out using various machine learning techniques to build an effective intrusion detection system. The developed model is then implemented and tested through simulation to evaluate its performance under different scenarios. Afterward, performance evaluation and analysis are conducted using relevant metrics to assess the effectiveness of the proposed model. Finally, the research concludes with conclusions and recommendations based on the findings to support future improvements and further studies.

4. RESULT AND DISCUSSIONS

Results

The proposed Anomaly-Based Intrusion Detection System (AbIDS) was evaluated using several machine learning models, including Decision Tree (DT), Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). The evaluation was conducted using standard performance metrics such as accuracy, precision, recall, F1-score, and false positive rate (FPR).

The experimental results indicate that deep learning-based models outperform traditional machine learning approaches. Specifically, the LSTM model achieved the highest performance due to its ability to capture temporal patterns in network traffic data, followed closely by CNN, which performed well in recognizing complex traffic patterns.

Table 1. Performance Comparison of IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
DT	88.5	87.2	86.9	87.0	8.5
SVM	91.3	90.5	89.8	90.1	6.7
CNN	95.6	94.8	95.2	95.0	3.9
LSTM	96.8	96.1	96.5	96.3	3.2

The results show that LSTM achieved the highest accuracy of 96.8%, followed by CNN at 95.6%. In terms of false positive rate, LSTM also demonstrated the lowest value at 3.2%, indicating better reliability in distinguishing normal and malicious traffic.

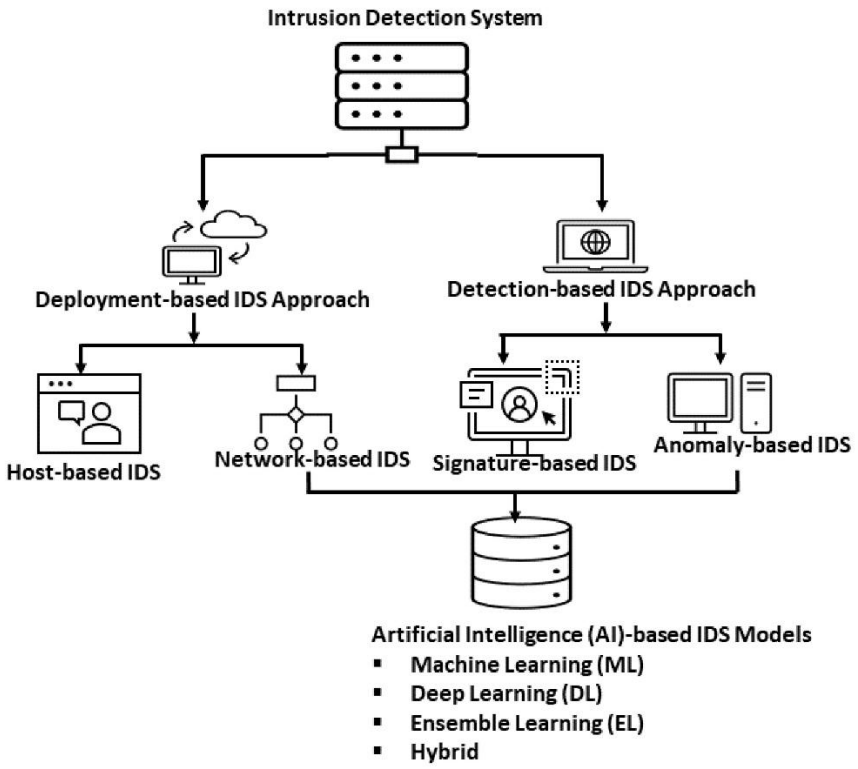


Figure 2. Accuracy Comparison of IDS Models

The graph illustrates that deep learning models (CNN and LSTM) significantly outperform traditional models (DT and SVM), highlighting their effectiveness in handling complex intrusion patterns.

Discussion

The findings of this study demonstrate that machine learning-based IDS, particularly deep learning models, provide substantial improvements over traditional approaches. The superior performance of LSTM can be attributed to its ability to model sequential dependencies in network traffic, which is essential for detecting time-based attack patterns. Similarly, CNN shows strong performance due to its capability in extracting spatial features from high-dimensional data. Compared to traditional rule-based or signature-based IDS, the proposed AbIDS model is more adaptive and capable of detecting unknown or zero-day attacks. This aligns with the literature, which suggests that anomaly-based approaches are more suitable for dynamic and evolving network environments. However, despite the high accuracy, several challenges remain. One of the main issues is the computational complexity of deep learning models, which may impact real-time performance in large-scale networks. Additionally, although the false positive rate is reduced, it is not completely eliminated, which may still require manual verification by security analysts.

The implementation of incremental learning in this study also contributes to system adaptability, allowing the IDS to update its knowledge with new data without retraining from scratch. This is particularly important in modern cybersecurity environments where new attack patterns continuously emerge. Overall, the results confirm that integrating machine learning, especially deep learning techniques, into IDS significantly enhances detection performance, reduces false positives, and improves the system's ability to operate in real-time conditions. These findings support the proposed approach as a viable solution for modern network security challenges.

5. CONCLUSION

This study has successfully developed and evaluated an Anomaly-Based Intrusion Detection System (AbIDS) using various machine learning and deep learning techniques to enhance network security. The results demonstrate that machine learning-based approaches significantly improve intrusion detection performance compared to traditional methods, particularly in identifying both known and unknown attacks. Among the evaluated models, deep learning algorithms, especially Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN), achieved the highest performance in terms of accuracy, precision, recall, and F1-score, while also maintaining a lower false positive rate. This indicates that deep learning models are more effective in capturing complex and dynamic patterns in network traffic data.

Furthermore, the integration of an incremental learning approach enhances the adaptability of the system, allowing it to respond to emerging threats without requiring complete retraining. This capability is essential for maintaining effectiveness in rapidly evolving cybersecurity environments. Despite these advantages, challenges such as computational complexity and the presence of false positives remain important considerations for real-world implementation. Therefore, future research should focus on optimizing model efficiency, reducing false alarm rates, and improving real-time processing capabilities. In conclusion, the proposed machine learning-based IDS provides a robust, adaptive, and effective solution for modern network security, making it a promising approach for protecting digital infrastructure against increasingly sophisticated cyber threats.

REFERENCES

[1] K. Mahanta and H. B. Maringanti, "Machine learning approaches for intrusion detection: Enhancing cybersecurity and threat mitigation," in *Cognitive Machine Intelligence: Applications, Challenges, and Related Technologies*, 2024, pp. 199–218. doi: 10.1201/9781003500865-11.

[2] A. S. Jaradat, M. M. Barhoush, and R. B. Easa, "Network intrusion detection system: Machine learning approach," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 25, no. 2, pp. 1151–1158, 2022, doi: 10.11591/ijeecs.v25.i2.pp1151-1158.

[3] V. Kathiresan, S. Karthik, P. Divya, and D. P. Rajan, "A comparative study of diverse intrusion detection methods using machine learning techniques," in *2022 International Conference on Computer Communication and Informatics (ICCCI 2022)*, 2022. doi: 10.1109/ICCCI54379.2022.9740744.

[4] A. R. Ugale and A. D. Potgantwar, "Anomaly based intrusion detection through efficient machine learning model," *Int. J. Electr. Electron. Res.*, vol. 11, no. 2, pp. 616–622, 2023, doi: 10.37391/ijeer.110251.

[5] R. Udayakumar, D. Balakrishnan, Y. V Reddy, P. B. E. Prabhakar, and A. Thilaka, "Machine learning based intrusion detection system," in *Proceedings of the International Conference on Technological Advancements in Computational Sciences (ICTACS 2023)*, 2023, pp. 197–205. doi: 10.1109/ICTACS59847.2023.10389883.

[6] V. W. Samawi, S. A. Yousif, and N. M. G. Al-Saidi, "Intrusion detection system: An automatic machine learning algorithms using {Auto-WEKA}," in *2022 IEEE 13th Control and System Graduate Research Colloquium (ICSGRC 2022)*, 2022, pp. 42–46.

doi: 10.1109/ICSGRC55096.2022.9845166.

[7] G. R. Deng *et al.*, “Application research of intrusion prevention system in emergency platform network,” in *Advances in Intelligent Systems and Computing*, 2020, pp. 1158–1166. doi: 10.1007/978-3-030-15235-2_153.

[8] D. Ali, A. M. Tripathi, and K. Saini, “A study on network security and cryptography,” in *Proceedings of the IEEE 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N 2024)*, 2024, pp. 511–514. doi: 10.1109/ICAC2N63387.2024.10894984.

[9] B. Nithya, V. Ilango, and S. Mohan Kumar, “Cryptographic system models and algorithms for network security,” *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1, pp. 1177–1183, 2019.

[10] M. Abdulkadhim and S. Hasan, “Boosting the network performance using two security measure scenarios for service provider network,” *Iraqi J. Sci.*, pp. 174–179, 2021, doi: 10.24996/ijs.2021.SI.1.24.

[11] Ö. Aslan, S. S. Aktu\ug, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,” *Electron.*, vol. 12, no. 6, p. 1333, 2023, doi: 10.3390/electronics12061333.

[12] O. Alshamsi, K. Shaalan, and U. Butt, “Towards securing smart homes: A systematic literature review of malware detection techniques and recommended prevention approach,” *Inf.*, vol. 15, no. 10, p. 631, 2024, doi: 10.3390/info15100631.

[13] K. Mohamed Shalman Kursheeth, T. Sree, D. Sendil Vadivu, Y. S. S. Harsha, and N. Rajagopalan, “Suricata-based intrusion detection and isolation system for local area networks,” in *Proceedings of the International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT 2024)*, 2024. doi: 10.1109/IConSCEPT61884.2024.10627890.

[14] H. Hendrawan, P. Sukarno, and M. A. Nugroho, “Quality of service ({QoS}) comparison analysis of {Snort IDS} and {Bro IDS} application in software defined network ({SDN}) architecture,” in *2019 7th International Conference on Information and Communication Technology (ICoICT 2019)*, 2019. doi: 10.1109/ICoICT.2019.8835211.

[15] A. Sahu, Z. Mao, K. Davis, and A. E. Goulart, “Data processing and model selection for machine learning-based network intrusion detection,” in *IEEE International Workshop on Communications Quality and Reliability (CQR 2020)*, 2020. doi: 10.1109/CQR47547.2020.9101394.

[16] D. G. Bhatti and P. V Virparia, “Soft computing-based intrusion detection system with reduced false positive rate,” in *Design and Analysis of Security Protocol for Communication*, 2020, pp. 109–139. doi: 10.1002/9781119555759.ch5.

[17] F. E. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, “Intrusion detection systems using long short-term memory ({LSTM}),” *J. Big Data*, vol. 8, no. 1, p. 65, 2021, doi: 10.1186/s40537-021-00448-4.

[18] K. Azarudeen, S. Harish Kumar, T. V Aswin Vijay, P. Thirukumaran, and V. S. Barath Balaji, “Intrusion detection system based on pattern recognition using {CNN},” in *International Conference on Sustainable Computing and Smart Systems (ICSCSS 2023)*, 2023, pp. 567–574. doi: 10.1109/ICSCSS57650.2023.10169670.

[19] M. Arief and S. H. Supangkat, “Comparison of {CNN} and {DNN} performance on intrusion detection system,” in *Proceedings of the 9th International Conference on ICT for Smart Society (ICISS 2022)*, 2022. doi: 10.1109/ICISS55894.2022.9915157.

[20] A. Heryanto, D. Stiawan, M. Y. Bin Idris, M. R. Bahari, A. A. Hafizin, and R. Budiarto, “Cyberattack feature selection using correlation-based feature selection method in an intrusion detection system,” in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2022)*, 2022. doi: 10.23919/EECSI56542.2022.9946449.

[21] F. A. P. Kuswara, H. H. Nuha, and V. Suryani, “Intrusion detection system using incremental learning method,” in *2023 11th International Conference on Information and Communication Technology (ICoICT 2023)*, 2023, pp. 588–593. doi: 10.1109/ICoICT58202.2023.10262799.