Evaluation of the Effectiveness of *Intrusion Prevention Systems* (IPS) in Mitigating *Modern Network Threats*: A Systematic Review

1st Sumitra Adriansyah
Informatics Department
UIN Sunan Gunung Djati Bandung
West Java, Indonesia
sumitraadriansyah@gmail.com

***Abstract-This study* aims to evaluate the development of network intrusion detection and prevention systems (IDS/IPS) with a systematic review approach of the latest methods and algorithms. The analysis shows that complex cyber threats such as DDoS, brute force, and SQL injection require intelligent solutions based on artificial intelligence (AI) and machine learning. Approaches based on Suricata, Fail2ban, and the integration of real-time notification systems have proven effective in addressing cyber threats. The results show that algorithmic innovation, modern datasets, and big data-driven systems can significantly improve network response and security, with the potential to adapt to evolving threats.**

***Index Terms-Intrusion* Prevention Systems, Network Security, Threat Mitigation, Cybersecurity, Systematic Review**

I. Introduction

In this rapidly evolving digital era, computer network security has become a major concern for organizations around the world. As the reliance on information and communication technology continues to increase, cyber threats are becoming more sophisticated and dangerous. According to the latest Cisco Annual Internet Report for 2028 to 2023, the number of devices connected to the internet is expected to reach 29.3 billion by 2023, with significant growth from 18.4 billion in 2018 [1]. With this rapid growth, it provides a major challenge in the aspect of network security, especially in the face of cyber threats that continue to be more sophisticated. Intrusion Prevention System (IPS) has emerged as one of the critical components in modern network security architecture that is a solution dealing with cyber threats. Intrusion Prevention System (IPS) is a network security tool that can detect and prevent attacks by examining network traffic with rules. For additional protection, IPS can block malicious packets and log suspicious activities [2]. Meanwhile, Intrusion Detection Systems (IDS) is a very important tool for network security, which is designed to detect intrusions. and respond to unauthorized access or attacks [3]. In contrast to intrusion detection systems (IDS) that only monitor and report suspicious activity, IPS has the ability to actively prevent or block detected threats in real-time. The development of cyber threats in recent years has shown an alarming increase. Based on the Indonesian National Cyber and Crypto Agency (BSSN), stated that there were 74 million traffic anomalies from January to May 2024, of which 44 million anomalies were detected as malware activity, and the rest were trojans [4]. The data shows that there a need for increased cybersecurity in an increasingly technological era.

This is state-of-the-art.

The implementation of IPS in this modern network environment faces various challenges. These challenges are, for example, where cybersecurity is increasingly complex and continues to increase, making it difficult for conventional IPS to keep up with evolving threats [5]. Then with a dynamic network environment, it turns out to require variability in network traffic and attack data assimilation which can complicate detection efforts, this is because IPS must adapt to changing conditions [5].

This systematic review aims to evaluate the effectiveness of IPS technology in dealing with Modern Network Threats. The focus of this research is specifically on the adaptability of the system to new threats and its impact on overall network performance.

II. Literature Review

In recent years, research on the effectiveness of Intrusion Prevention System (IPS) in overcoming modern network threats has been conducted. Many studies have examined the effectiveness of using this method in preventing cyber attacks.

Maulani, I, E, et. al raised issues related to increasingly complex cyber threats, thus requiring an effective IDS. The research uses the method

In-depth interviews with network and human experts to understand system requirements. It was found that IDS is able to be the first line of defense that detects suspicious activity and protects the network [6].

Kurniawan, A, et. al also highlighted that threats such as port scanning, brute force, and DDoS. These threats can be handled effectively in improving network security, by Suricata IPS which has been tested to detect these threats [7].

Research conducted by Deepaa Selva et. al also succeeded in building a smarter network security system using algorithms such as genetics and neural networks. The results of the study stated that the intrusion detection system is more adaptive and accurate, so that it can handle evolving threats [8].

Deinega et.al also managed to find a system that successfully detects threats with high accuracy, beyond conventional, to overcome the limitations of traditional systems by integrating artificial intelligence algorithms, such as neural networks and fuzzy logic [9].

Faula Tanang Anugrah et al, in their research focused on SQL Injection attack detection using Suricata. The results show Suricata effectively detects various types of attacks, although there is an increase in server response time [2].

Fazar Dawamsyach et al, in their research developed an IPS system with Fail2ban to prevent brute force and DDoS attacks. The results show that Fail2ban is effective in detecting and counteracting threats, despite the impact on CPU and memory performance [10]. Rayco William, et al. Stated in his research that using IPS with Suricata is used to handle DDoS attacks and ping attacks. The system features notifications via Telegram, which speeds up the response to threats and improves server security. [11].

Patrick Vanin et al. The research focuses on improving IDS with hybrid methods and algorithms such as SVM and CNN. This approach improves accuracy, although it still uses old datasets that are less relevant to modern environments [12].

Farah Jemili in her research developed a detection system based on Big Data and cloud communications equipped with an expert system to provide more specific security recommendations. The result is an increase in the accuracy of threat detection and prediction [13].

Michael Hart, et. al, examined the design of big data environments to deliver critical inputs and outputs by designing, configuring, and evaluating multiple architectural layers. Using a design science approach, the research developed artifacts to solve business problems, including the placement of Intrusion Detection and Prevention Systems (IDPS) in evolving network architectures. The research methodology involved eight steps to design, test, and benchmark the system across different network environment. As a result, they managed to create a mature model for IDPS, with high effectiveness in handling attacks, such as DDoS, on perimeter-based architectures. This research also revealed the importance of security system design optimization and implementation limitations influenced by environmental factors as well as the number of architectures tested [14].

III. Methodology

The research methodology used in this study is to use a systematic review approach to evaluate the effectiveness of the Intrusion Prevention System (IPS) system in mitigating modern network threats. This research involves the following stages:

A. Research Design

This research uses a systematic review method that aims to collect, analyze, and synthesize research results related to Intrusion Prevention System (IPS) from various relevant sources.

B. Data Collection Process

The data collected in this study came from journals, conferences, and trusted scientific publications, using a combination of keywords Intrusion Prevention System, Modern Network Threats, IPS effectiveness, Machine Learning in IPS, and Network Security. The articles selected were published between 2021 and 2024.

C. Problem Identification

The main issues raised in this research include:

- The complexity and diversity of modern network threats such as DDoS, *brute force*, and SQL Injection.
- The need for integration of intelligent algorithms to improve intrusion detection accuracy.
- Challenges in deploying IPS in real environments, including the *trade-off* between security and performance.

D. Framework Analysis

This research then evaluates the effectiveness of Intrusion Prevention Systems (IPS) frameworks in Mitigating Modern Network Threats. This was done by identifying and analyzing relevant past research to understand the effectiveness of different types of IPS in handling different types of threats such as DDoS, SQL Injection, port scanning, and brute force attacks. The focus of this framework is on the types of threats that can be detected and prevented by IPS and analyzing the effectiveness of IPS in responding to these threats. Then, it measures IPS performance with parameters such as response time, detection accuracy, and impact on system performance. Finally, it assesses the technologies and algorithms used in each study to improve IPS capabilities.

E. *Data Analysis*

The data analysis process was conducted by systematically reviewing the results of ten selected studies. Each article was analyzed based on, the problem, methodology, and research results obtained then loaded into key findings, which were then categorized to identify common patterns and significant findings related to the effectiveness of IPS in mitigating modern network threats.

F. *Validation of Results*

The findings in the literature study were compared with each other to validate the effectiveness of the proposed solution. This evaluation includes comparison with the methods used as well as recent innovations in IPS systems or IPS accuracy and efficiency.

IV. Results and Discussion

The results of the analysis of the 10 evaluated studies are shown in Table. 1. below, which provides an overview of the findings from each study.

TABLE I
Results of Analysis of Recent Findings of Effectiveness Research Intrusion Prevention Systems (IPS) in Mitigating Modern Network Threats

No.	Researcher	Key Findings
1	Isma Elan Maulani, Aldo Faisal Umam	IPS acts as a line of defense per- First, it helps detect suspicious activity and mitigate the impact of an .
2	Andhika Kurniawan, Lukman Medriavin Silalahi	Suricata is effective in detecting attacks port scanning, brute force, and DDoS.
3	Deepaa Selva et al.	Intelligent algorithms, including neural networks and genetic algorithms, improving intrusion detection and prevention.
4	T. S. Deinega et al.	Neural network and logic-based models fuzzy improves reliability and efficiency in intrusion detection.
5	Faula Tanang Anugrah et al.	Suricata is effective in detecting SQL Injection, with a slight decrease in response time.
6	Fazar Dawamsyach et al.	Fail2ban is effective in overcoming attacks DDoS and brute force, although there is a trade-off in performance.
7	Rayco William et al.	Suricata is effective in detecting DDoS, ping attacks, and port scanning, with automatic no- tification via Telegram.
8	Patrick Vanin et al.	Hybrid and ensemble approaches lead to on more accurate detection, even though it still uses old datasets.
9	Farah Jemili	Big Data-based detection system and computation cloud has high precision and accuracy in intrusion detection.
10	Farah Jemili	IDPS placement in big data architecture can increase the effectiveness of intrusion detection and prevention systems.

The results of the analysis of the literature review, it can be concluded that, research related to the effectiveness of Intrusion Prevention Systems (IPS) in dealing with modern network threats show solutions, it turns out that IPS has an important role in improving overall network security.

A. *Network Threat Detection and Prevention*

IPS has proven to be effective in detecting and preventing various types of threats, such as brute force attacks, port scanning, DDoS, and SQL injection. Systems using systems such as Suricata, which have been used in several studies, were found to successfully block malicious activity with high accuracy, thus showing that IPS has the ability to reduce the impact of attacks that could previously harm the network.

For example, in tests involving Suri- cata against port scanning and brute force attacks, the system was able to respond to threats quickly and accurately. In fact, this research highlights the effectiveness of support algorithms such as genetic algorithms, neural networks, and fuzzy logic in detecting more complex and unpredictable attack patterns.

B. *Improved Detection Speed and Accuracy*

The approach of combining *machine learning* methods and artificial intelligence algorithms has shown significant results. Systems that use *super- vised learning* and algorithms such as neural networks have achieved up to 98% accuracy in detecting threats. This not only helps speed up response times but also improves the system's ability to adapt to evolving attack patterns.

C. *Adaptation to Modern Threats*

The results of the previous research revealed that it is important to use more representative datasets and develop models that can adaptively learn from new network traffic data, because one of the weaknesses of traditional detection systems is the dependence on old datasets that are irrelevant to modern network traffic. To handle *big data* and provide real-time security recommendations, systems based on *big data* and cloud computing are emerging.

D. *Operational Efficiency*

One of the biggest challenges in IPS deployment is finding a balance between network security and network performance. The previous research showed that although systems such as Suricata significantly improved security, there was a trade-off in the form of increased latency and resource consumption. For example, when facing a SQL injection attack, the server response time increased slightly, although the threat was well managed.

However, with intelligent rule selection and parameter optimization such as maxretry, the system can provide optimal protection without drastically compromising network performance.

E. Limitations and Areas for Improvement

Although the results show many advantages, there are still new challenges that need to be overcome. The current system still has weaknesses in dealing with certain types of more specific attacks or new attacks that have not yet been recognized. Another challenge is the high resource requirements, especially for the implementation of a system based on artificial intelligence algorithms. Although the results are promising, the system still needs further optimization to be implemented on a larger scale.

V. Conclusion

Based on the research results that have been reviewed in this research, it can be concluded that the Intrusion Prevention System is a very important component in the modern network security ecosystem. By integrating intelligent algorithms and machine learning approaches, IPS can effectively detect, deter, and respond to a variety of evolving network threats. However, there is still a need for continuous improvement in detection methods, resource efficiency, and the development of more relevant datasets in the face of future challenges.

Acknowledgment

The authors would like to thank the Department of Informatics Engineering of UIN Sunan Gunung Djati Bandung for the support and provision of resources that were very helpful in completing this research. Special thanks go to Mr. Gitarja Sandi S.T., M.T., who provided valuable guidance and advice during the research process. His contributions greatly enriched the quality of this research.

References

[1] Cisco, "Cisco annual internet report (2018-2023) white paper," 2020, accessed: [23/12/2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] F. Tanang Anugrah, S. Ikhwan, and J. Gusti A.G, "Implementation of intrusion prevention systems (ips) using suricata for sql injection attacks," *Techne´ : Scientific Journal of Electrotechnics*, vol. 21, no. 2, p. 199-210, Sep. 2022. [Online]. Available: https://ojs.jurnaltechne.org/index.php/techne/article/view/320

[3] A. M. Affan, "Evolving adversarial training (eat) for ai-powered intrusion detection systems (ids)," *American Journal of Computer Science and Technology*, vol. 7, no. 3, pp. 115-121, 2024. [Online]. Available: https://doi.org/10.11648/j.ajcst.20240703.16

[4] cnn indonesia team. (2024) Bssn detects 44 million malware activities by May 2024. Accessed: 23/12/2024. [Online]. Available: https://www.cnnindonesia.com/teknologi/20240516184354- 185-1098626/bssn-deteksi-44-juta-aktivitas-malware-hingga-mei-2024

[5] H. Han, H. Kim, and Y. Kim, "An efficient hyperparameter control method for a network intrusion detection system based on proximal policy optimization," *Symmetry*, vol. 14, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2073-8994/14/1/161

[6] I. Elan Maulani and A. faisal umam, "Evaluation of the effectiveness of intrusion detection system in ensuring network security," *Journal of Social Technology*, vol. 3, no. 8, p. 662-667, Aug. 2023. [Online]. Available: https://sostech.greenvest.co.id/index.php/sostech/article/view/907

[7] L. M. Silalahi and A. Kurniawan, "Network security analysis using intrusion prevention system (ips) with traffic behavior method," *Electrician: Journal of Electrical Engineering and Technology*, vol. 17, no. 1, pp. 71-76, Jan. 2023. [Online]. Available: https://electrician.unila.ac.id/index.php/ojs/article/view/2296

[8] D. Selva, B. Nagaraj, D. Pelusi, R. Arunkumar, and A. Nair, "Intelligent network intrusion prevention feature collection and classification algorithms," *Algorithms*, vol. 14, no. 8, 2021. [Online]. Available: https://www.mdpi.com/1999-4893/14/8/224

[9] T. Deineha and I. Svatovskiy, "Research of using the artificial intelligence algorithms in intrusion detection/prevention systems," *Bulletin of V.N. Karazin Kharkiv National University, series Mathematical modeling. Information technology. Automated control systems*, vol. 54, pp. 16-26, Jun. 2022. [Online]. Available: https://periodicals.karazin.ua/mia/article/view/22222

[10] F. Dawamsyach, I. Ruslianto, and U. Ristian, "Implementation of ips (intrusion prevention system) fail2ban on server for ddos and brute force attacks," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, pp. 149-149, 2023.

[11] R. D. William, I. Ruslianto, and U. Ristian, "Implementation of intrusion prevention system (ips) as a website-based server security system and mobile application," *CESS (Journal of Computer Engineering, System and Science)*, vol. 8, no. 1, pp. 123-123, 2023.

[12] P. Vanin, T. Newe, L. L. Dhirani, E. O'Connell, D. O'Shea, B. Lee, and M. Rao, "A study of network intrusion detection systems using artificial intelligence/machine learning," *Applied Sciences*, vol. 12, no. 22, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/22/11752

[13] F. Jemili, "Active intrusion detection & prediction based on temporal big data analytics," https://doi.org/10.21203/rs.3.rs-2838468/v1, Apr. 2023, pREPRINT (Version 1).

[14] M. Hart, R. Dave, and E. Richardson, "Next-generation intrusion detection and prevention system performance in distributed big data network security architectures," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2023.01409103