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
Jawa Barat, Indonesia
sumitraadriansyah@gmail.com

***Abstract*—This research aims to evaluate the development of network intrusion detection and prevention systems (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 innovations, modern datasets and big data-driven systems can significantly improve network responsiveness and security, with the potential to improve network performance.**

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

I. Introduction

In this rapidly evolving digital age, 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 become more sophisticated.

Intrusion Prevention System (IPS) has emerged as one of the critical components in modern network security architecture that is a solution to modern 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 activity [2]. While Intrusion Detection Systems (IDS) is a very important tool for network security, which is designed to detect and respond to unauthorized access or attacks [3]. So in contrast to intrusion detection systems (IDS) that only monitor and report suspicious activity, this IPS has the ability to actively prevent or block threats detected in real-time.

The development of cyber threats in recent years has shown an alarming increase. According to Indonesia's National Cyber and Crypto Agency (BSSN), 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 is a need to improve cybersecurity in this era of increasingly sophisticated technology.

The implementation of IPS in this modern network environment faces various challenges. Such challenges include where cyber security is increasingly complex with increasing, making it difficult for conventional IPS to keep up with the growing threat [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 conditions that are constantly changing [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 their 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 study used an in-depth interview method with network and security experts to understand system requirements. So that the results found are that IDS is able to become 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 state that the intrusion detection system is more adaptive and accurate, so that it can handle the evolving threats [8].

Deinega et.al also managed to find a system that successfully detects threats with high accuracy, beyond the 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 that 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, although there is an 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 the modern environment [12].

Farah Jemili in research conducted in developing a Big Data-based detection system and cloud computing equipped with an expert system to provide more specific security recommendations. The result is an increase in the accuracy of detection and prediction of threats [13].

Michael Hart, et. al, examined the design of big data environments to produce 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 an evolving network architecture. The research methodology involved eight steps to design, test and benchmark the system in various network environments. 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. The 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 Intrusion Prevention System (IPS) systems in mitigating modern network threats. This research involved the following stages:

A. Research Design

This research uses a systematic review method that aims to collect, analyze, and synthesize research results related to the 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 selected articles are published in the range of 2021 to 2024.

C. Identifikasi Masalah

Permasalahan utama yang diangkat dalam penelitian ini meliputi:

- 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 framework effectiveness of Intrusion Prevention Systems (IPS) 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, by assessing the technologies and algorithms used in each study to improve the capabilities of the IPS.

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 a key finding, which was 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 comparisons with 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 Research Findings on the Effectiveness of Intrusion Prevention Systems (IPS) in Mitigating Modern Network Threats

No.	Researcher	Key Findings
1	Isma Elan Maulani, Aldo Faisal Umam	IPS acts as the first line of defense, helping to detect suspicious activity and mitigate the impact of attacks.
2	Andhika Kurniawan, Lukman Medriavin Silalahi	Suricata is effective in detecting port scanning, brute force, and DDoS attacks.
3	Deepaa Selva et al.	Intelligent algorithms, including neural networks and genetic algorithms, improve intrusion detection and prevention.
4	T. S. Deinega et al.	Neural network and fuzzy logic-based models improve 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 dealing with DDoS and brute force attacks, 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 notifications via Telegram.
8	Patrick Vanin et al.	Hybrid and ensemble approaches lead to more accurate detection, although still using old datasets.
9	Farah Jemili	Big Data and cloud computing-based detection systems have high precision and accuracy in intrusion detection.
10	Farah Jemili	Placement of IDPS 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 System (IPS) in dealing with modern network threats shows a solution, it turns out that this 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 such as Suricata, which have been used in several studies, were found to block malicious activity with high accuracy, demonstrating that IPS has the ability to reduce the impact of attacks that would otherwise harm the network.

For example, in tests involving Suricata 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 supporting algorithms such as genetic algorithms, neural networks, and fuzzy logic in detecting more complex and unpredictable attack patterns.

B. Increased Speed and Accuracy of Detection

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

C. Adaptation to Modern Threats

The research conducted in the previous study 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 not relevant 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 optimisation of parameters 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 recognised. Another challenge is the high resource requirement, especially for the implementation of a system based on artificial intelligence algorithms. Although the results are promising, the system still needs further optimisation to be implemented on a larger scale.

V. Conclusion

Based on the research results that have been reviewed in this study, 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 approaches with machine learning, it turns out that IPS can effectively detect, prevent, and respond to various network threats that continue to grow. 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 are very helpful in completing this research. Special thanks go to Mr Gitarja Sandi S.T., M.T., who provided valuable guidance and advice throughout 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, "Implementasi intrusion prevention system (ips) menggunakan suricata untuk serangan sql injection," *Techné : Jurnal Ilmiah Elektroteknika*, 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] tim cnn indonesia. (2024) Bssn deteksi 44 juta aktivitas malware hingga mei 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, "Evaluasi efektivitas sistem deteksi intrusi dalam menjamin keamanan jaringan," *Jurnal Sosial Teknologi*, 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, "Analisis keamanan jaringan menggunakan intrusion prevention system (ips) dengan metode traffic behavior," *Electrician : Jurnal Rekayasa dan Teknologi Elektro*, 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