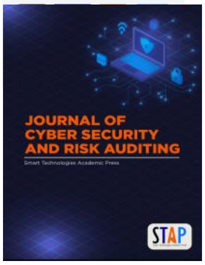

JOURNAL OF CYBER SECURITY AND RISK AUDITING
Smart Technologies Academic Press
STAP

STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process

Sokroeurn Ang, [1] **Mony Ho,** [1] **Sopheaktra Huy,** [1] **Midhunchakkaravarthy Janarthanan** [1]

[1] *AI Computing and Multimedia Department, Lincoln Graduate Program, Doctor in Cybersecurity, Lincoln University College, Malaysia*

ARTICLE INFO

Article History

Received: 01-05-2025
Revised: 30-06-2025
Accepted: 01-05-2025
Published: 02-07-2025

Vol.2025, No.3

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.3.10

Corresponding author.
Email:
angsokroeurn.phdscholar@lincoln.edu.my

ABSTRACT

Intrusion detection system (IDS) and intrusion prevention system (IPS) are crucial for protecting cyberattacks that target organizational information systems, IDS is focusing on detecting cyberattacks while IPS is focusing on preventing cyberattack. The research examines the limitations of IDS and IPS in detecting and preventing threats, highlighting that both systems rely on signature and anomaly-based detection methods. However, these detection techniques require significant enhancements, as current implementations in IDS and IPS may not effectively address all threats. The main objective of this study is to discover the limitation feature of IDS and IPS in detecting and preventing threats. The data collection and analysis are using a combination of quantitative and qualitative approaches, based on an in-depth review of research and review articles. The analysis shows that attackers can exploit information systems due to the absence of latest signatures and anomaly-based detection in intrusion detection systems (IDS) and intrusion prevention systems (IPS). The findings recommend that cybersecurity professionals should regularly update and verify both signature-based and anomaly-based detection mechanisms, as well as implement both network-based and host-based level to ensure that IDS and IPS can effectively detect and prevent threats in real time.

Keywords: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Signature, Anomaly, Cyberattack, Cyber threat.

How to cite the article
Ang, S., Huy, S., & Janarthanan, M. (2025). Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process. Journal of Cyber Security and Risk Auditing, 2025(3), 77–88. https://doi.org/10.63180/jcsra.thestap.2025.3.10

1. Introduction

As cyberattacks grow in complexity and frequency, the demand for robust security measures to safeguard organizational IT infrastructure becomes increasingly crucial. In response, organizations adopt Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as essential technologies for monitoring and protecting cybersecurity infrastructures [1].

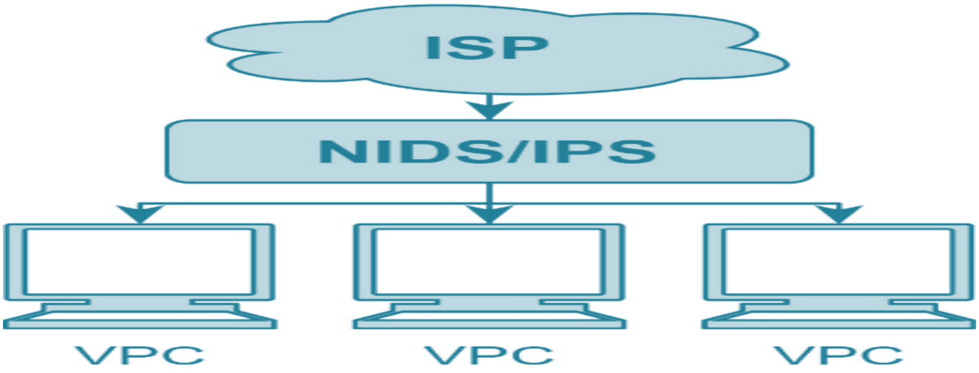

Figure 1: Network based intrusion detection and prevention system.

Based on Figure 1, shows that the implementation of IDS and IPS depend solely on network-based IDS and IPS systems. When the computers disconnect from the network, the attacker definitely can exploit the computers without detecting and preventing IDS and IPS.

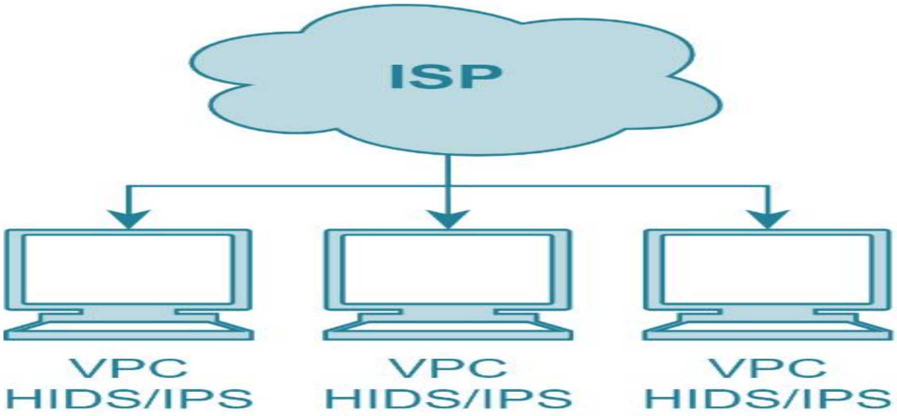

Figure 2: Host based intrusion detection and prevention system.

According to Figure 2, demonstrates that the implementation of IDS and IPS depend solely on host-based IDS and IPS systems. When the attacker targets to exploit through the network, the attacker might be able to exploit the computers without detecting and preventing IDS and IPS.

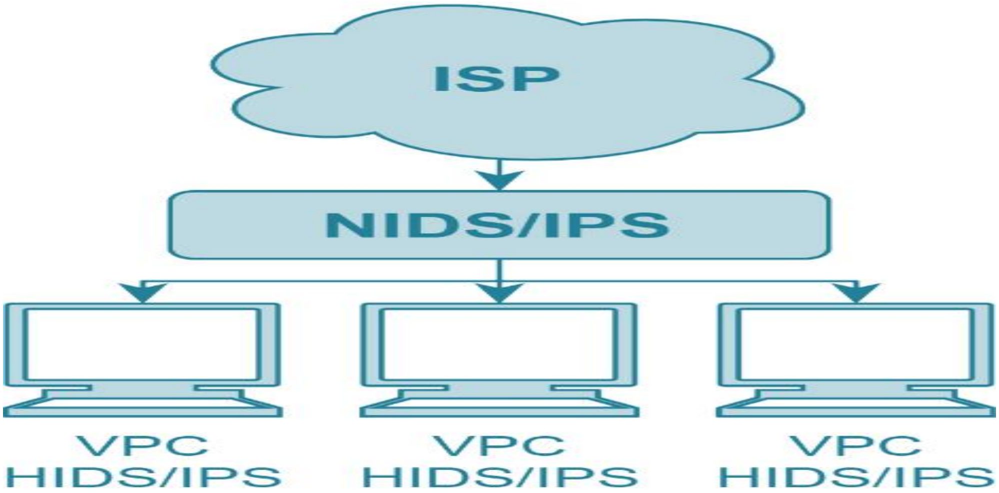

Figure 3: Network and host-based intrusion detection and prevention system.

Regarding Figure 3, illustrates a secure implementation of IDS and IPS, while it consists of network-based IDS and IPS as well as host-based IDS and IPS, it is considered as a secure implementation of cybersecurity control because it can manage cyberattacks from both network and host level [5]. An intrusion detection system (IDS) is a detective control mechanism that identifies cyberthreats and notifies malicious events to cybersecurity professionals. An intrusion prevention system (IPS) is a preventive control in nature that prevents cyberthreats from occurring in information system. IDS and IPS have signature and anomaly-based detection methods to detect and block cyberthreats. Signature based detection relies on common vulnerability exposures (CVE) and tends to produce fewer false positives. However, it is unable to detect or block new or unknown threats. Anomaly based detection generates more false positives, but it can identify and block new or unknown threats [2].

The balance between signature and anomaly-based detection mechanism remains a key consideration for organizations when implementing IDS and IPS technologies. Many organizations combine both mechanisms to enhance more comprehensive cybersecurity protection against both known and unknown threats [2]. By integrating signature and anomaly-based detection techniques, organizations can mitigate the risks associated with evolving cyberthreats effectively. Incorporating IDS and IPS solutions into a comprehensive cybersecurity monitoring process offers several advantages, including faster threat detection, more effective incident response, and strengthened protection of informational assets [3].

Although IDS and IPS offer several advantages for the cybersecurity monitoring process, especially in security operation centers (SOC), they also produce additional concerns, including false positives, outdated signatures, inability to detect and protect against new threats, and the complexity of managing rules. This study addresses the challenges with deploying and managing IDS and IPS solutions and explores best practices for improving their effectiveness on detecting and preventing cyberthreat [4].

This paper discusses the function of IDS and IPS in modern cybersecurity frameworks, focusing on their combined use to strengthen cybersecurity monitoring processes and provide a proactive approach against evolving cyber threats. Additionally, this study explores the features of security vulnerability detection and prevention to develop a robust framework for cybersecurity detection and prevention [5].

It also aims to provide some recommendations to improve IDS and IPS to contribute to early threat detection, incident response, and overall security posture enhancement. These suggestions focus on optimizing the cybersecurity monitoring process, ensuring that organizations can better detect, prevent, and respond to potential cyberthreats in real time [5].

This article begins with an in-depth explanation of intrusion detection systems (IDS) and intrusion prevention systems (IPS), highlighting their definitions, key features, and role in cybersecurity. Following this foundational overview, the article explores the significant challenges with the implementation of IDS and IPS, including people, process, and technology. Through these discussions, the article contributes to a deeper understanding of

IDS and IPS systems, their challenges, and best practices for strengthening cybersecurity infrastructure monitoring processes effectively.

2. Methodology

This study plans to do a literature review as well as research article documents analysis, the focus on research articles and documents published, which discusses the challenges, benefits, and strategies to the use of IDS and IPS for the cybersecurity monitoring process. According to [8], [9] the literature review methods are essential for providing trends, patterns, and specific research areas, by establishing frameworks, theories, and research topics for next research on IDS and IPS.

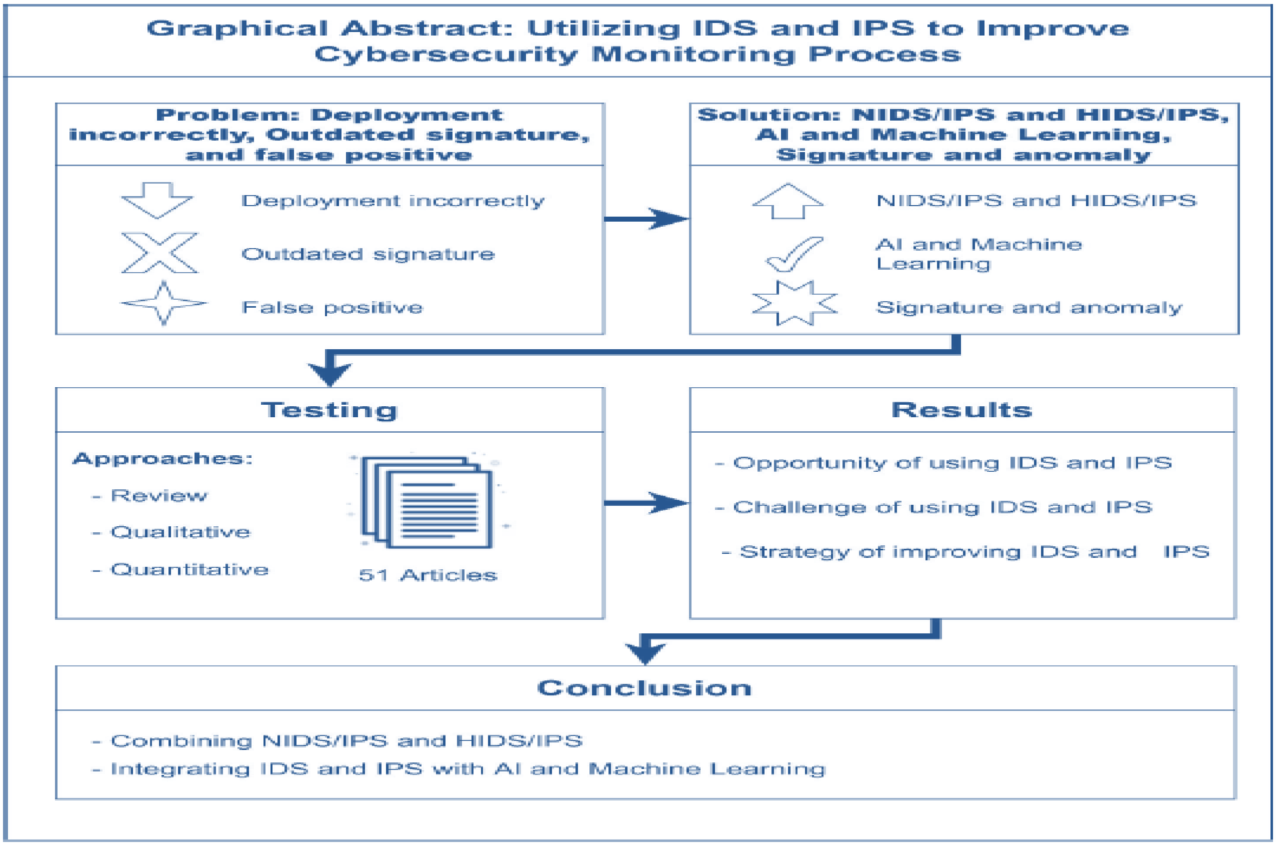
Graphical Abstract: Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process
Problem: Deployment incorrectly, Outdated signature, and false positive
Deployment incorrectly
Outdated signature
False positive
Solution: NIDS/IPS and HIDS/IPS, AI and Machine Learning, Signature and anomaly
NIDS/IPS and HIDS/IPS
AI and Machine Learning
Signature and anomaly
Testing
Approaches:
- Review
- Qualitative
- Quantitative
51 Articles
Results
- Opportunity of using IDS and IPS
- Challenge of using IDS and IPS
- Strategy of improving IDS and IPS
Conclusion
- Combining NIDS/IPS and HIDS/IPS
- Integrating IDS and IPS with AI and Machine Learning

Figure 4: Graphical abstract of utilizing IDS and IPS to improve cybersecurity monitoring process.

The following methods demonstrate the review:
Firstly, by conducting a search to identify relevant studies about IDS and IPS from various database sources, including Scopus, Google Scholar, IEEE, Science Direct, etc. Researchers use keywords to search, including challenge of using IDS and IPS, utilizing network-based IDS and IPS, utilizing host-based IDS and IPS, how to reduce false positives in IDS and IPS, benefit of using IDS and IPS, and strategy for improving IDS and IPS.
Secondly, researchers discuss and decide on the criteria of articles for the review:
1. Articles are written in English.
2. Articles publish in any form, including research articles, review articles, standard reports, and research reports.
Based on the review criteria with including a total of 51 articles. In addition, future studies should focus on overcoming these limitations.

3. Results and Discussion

This review divides the results into three categories: opportunities, challenges, and strategies regarding the use of IDS and IPS. The following sections discuss each category.

3.1 Opportunity of using IDS and IPS

As cyberthreats continue to evolve and increase rapidly, the need for a cybersecurity monitoring mechanism is essential especially IDS and IPS in order to manage security vulnerabilities effectively [1]. IDS and IPS enhance the cybersecurity monitoring process by examining malicious activities from security logs and the underlying motivations of security researchers in their improvement [1]. Drawing from a wide range of studies, we explore how these systems are vital not only for strengthening digital security but also for promoting a proactive cybersecurity culture. Additionally, highlighting opportunities in existing research and emphasizing the potential of IDS and IPS. Using a mixed methods research approach, this review seeks to offer a thorough overview of the benefits of IDS and IPS on software security, researcher involvement, and the broader cybersecurity landscape.

3.1.1 Various environment using IDS and IPS

Network based IDS and IPS deploy to control many endpoint devices and servers, [6] the study recommends using different data sources for signature and anomaly based in detecting and preventing cyberthreats. Additionally, as researchers can use different data sources from open source, enterprise source, public source, and standard source, it is also important to predefine those data sources by conducting training and testing to make sure it can detect and block known and unknown threats effectively [6]. In recent years, public data sources for detecting and protecting cyberthreats may exist while some data sources might not exist by involving research community and sharing scripts which could lead to more robust and diverse data sets in the future [6]. Network Intrusion Detection and Countermeasure Selection (NICE) is an innovative framework that uses Software-Defined Networking and attack graph analysis to detect and mitigate coordinated attacks in virtual cloud environments through programmable switches and specialized components such as NICE-A and a VM profiler. Performance evaluations show that NICE effectively enhances cloud security while minimizing disruptions to user traffic and service quality [28], [29], [35].

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are integral components of modern cybersecurity infrastructures. These systems help in the proactive detection and prevention of security threats within networks, providing real-time monitoring to detect and block cyberthreat [3]. IDS primarily monitors network traffic and raises alarms for potential threats, while IPS provides a step further by actively blocking malicious activities [3]. Effective deployment of both IDS and IPS systems significantly enhances an organization’s ability to defend against evolving cyberthreats, ensuring an improved cybersecurity posture properly [10].

A Network based intrusion prevention system (NIPS) to protect unauthorized activities. The NIPS designs to analyze network traffic streams, identify potential threats, and take automated actions to prevent cyberattacks. The effectiveness of NIPS in protecting against various types of attacks, including SYN floods, Denial of Service (DoS), and attacks targeting specific applications or infrastructure components [16].

These findings [17], [38] show the importance of IDS and IPS to detect and protect against brute force (login attempts detection) and other types of cyberthreats beyond brute force attacks, by protecting this attack, for the cybersecurity team needs to implement account lock out. Intrusion detection system (IDS) is significant for protecting information from cyberattacks, it typically classifies misuse of signature and anomaly detection, and it often treats as pattern recognition problems. This introduces the use of data mining and machine learning techniques to develop more effective IDS solutions [18]. The use of artificial intelligence and machine learning in network intrusion detection systems enhances the accuracy and efficiency of threat detection, enabling real time identification of sophisticated attacks. Additionally, deep learning techniques offer improved adaptability to evolving network traffic patterns, reducing false positives and increasing the overall effectiveness of cybersecurity systems [21]. An in details review of intrusion detection systems (IDS), focusing on feature selection, detection models, evaluation metrics, and datasets, and analyses techniques from 2008 to 2020 including machine learning (ML), deep learning (DL), and swarm and evolutionary (SWEVO) algorithms. It highlights the critical role of feature engineering in improving intrusion detection system accuracy and explores the limitations of commonly used datasets such as CIC-IDS-2017, which may not fully reflect modern and evolving cyberattack patterns. The paper also emphasizes the need for intelligent intrusion detection system response mechanisms capable of both accurate detection and real time defense, highlighting important directions for future research [22], [33], [39].

In cloud environments, it also uses network based and host-based IDS and IPS to detect and protect cyberthreats, including insider, flood, port scanning, and backdoor channel attacks [19], [41]. As DDOS attacks targets on cloud environments, it recommends using IDS, IPS, and DDOS protection to detect and block DDOS attacks on cloud environments to secure IT infrastructure [20], [41]. Industrial control system (ICS) uses IDS and IPS by enabling both security features signature based and anomaly-based detection to detect and protect cyberthreats target on ICS [23].

The Internet of Things (IoT) is rapidly growing and transforming various sectors, it also introduces numerous security vulnerabilities, and the increased interconnectivity of devices creates vulnerabilities that attackers can exploit, potentially compromising confidential data throughout the entire system. It is crucial to implement robust security measures, including IDS and IPS to protect the cyberattack on IoT devices [24].

The implementation of IDS/IPS using Snort on a Raspberry Pi 3B+ to enhance IoT security, demonstrating effective real-time detection of network attacks through pen testing with tools such as Nmap and Metasploit. The research highlights the accessibility of low-cost hardware for replicable security solutions and emphasizes the need to integrate robust defenses early in IoT system development [30].

Wireless networks are widely used by businesses to enable quick operations, but attackers can also exploit insecure Wi-Fi security protocols such as WEP and WPA. However, secure protocols such as WPA2 and WPA3 are resistant to cyberattack and offer a secure protection. In addition, with secure Wi-Fi security protocol, Wi-Fi networks also require security protection from IDS and IPS to detect and protect from malicious activities [26].

3.1.2 Reduce false positive by utilizing AI and Machine learning in IDS and IPS

The field of IDS and IPS provide significant advancements with technologies now leveraging machine learning, artificial intelligence, and advanced analytics to improve detection accuracy and reduce false positives [11]. Machine learning models are particularly useful in recognizing sophisticated attack patterns that may otherwise go undetected by traditional rule-based systems [12]. Similarly, deep learning techniques increasingly analyze large volumes of network traffic data and improve threat detection in real time [13]. [14], Highlights the shortcomings of traditional intrusion detection systems (IDS) in tackling the complex and continuously changing threats within IoT infrastructure. It presents machine learning as a good solution for intrusion detection, covering various approaches such as supervised, unsupervised, and deep learning methods. The discussion includes popular techniques such as artificial neural network (ANN), support vector machine (SVM), K-Nearest neighbor (KNN), and decision trees, as well as more advanced methods such as convolutional neural network (CNN), recurrent neural network (RNN), and generative adversarial network (GAN) [14], [40]. The importance of developing intrusion detection techniques that are robust in adversarial infrastructure by analyzing various machine learning and deep learning models applied to intrusion detection, such as support vector machine (SVM), decision trees (DT), and recurrent neural network (RNN) [15], [40].

Artificial intelligence (AI) and machine learning (ML) are addressing several of the challenges faced by traditional IDS/IPS systems. By using supervised and unsupervised learning algorithms, AI, and ML can improve detection accuracy, reduce false positives, and adapt to new attack patterns. These technologies offer the potential to create intelligent IDS and IPS systems that are more efficient, adaptive, and scalable [42], [47].

The deployment of IDS and IPS in modern networks faces numerous challenges, including performance issues, scalability, false positives, and adaptability to new threats. As networks continue to evolve, it is essential to explore new methodologies such as AI and machine learning to overcome these limitations. Researchers and practitioners must continue to refine IDS and IPS technologies to keep pace with the evolving threat landscape and ensure robust, efficient network security [47].

3.2 Challenge of using IDS and IPS

The existing signature based and anomaly-based detection methods face challenges in achieving both high performance and real time classification [7]. One of the standout contributions of this research is its inventive approach that combines both speed and accuracy in intrusion detection. This method enables the identification of advanced attacks, such as zero-day and various attacks, while still processing network traffic at line speeds. By utilizing packet-based classification for quick initial screening and then employing flow-based analysis for uncertain cases, the study introduces a fresh approach to network security [7]. The paper [27] outlines key challenges in current IDPS models, including difficulty detecting zero-day attacks and managing high false alarm rates. To overcome these, it proposes a hybrid framework combining anomaly and signature-based detection with risk factor analysis, and suggests future research directions for enhancing IoT security. One of the most significant challenges facing IDS and IPS are their ability to scale effectively as network traffic grows. Modern networks often handle millions of packets in real time, making it difficult for traditional IDS and IPS systems to detect and prevent threats without causing significant latency.

The IDS/IPS placement impacts the performance of big data systems in geographically distributed WAN, using a custom python based streaming application across various topologies including hub-and-spoke, custom-mesh, and full mesh. Results show that the custom-mesh topology provides the best balance of high-speed data streaming and reduced infrastructure costs, offering valuable insights into optimizing security and performance in geo-distributed big data environments [29].

A taxonomy-based analysis of privacy concerns in IDS, categorizing sensitive data into input, built-in, and generated types, and surveying research prototypes addressing privacy through various techniques such as encryption and pseudonymization. A key insight is the challenge of balancing privacy, performance, and precision-highlighting the need for innovative approaches that minimize trade-offs among these critical factors [31].

In environments such as cloud computing and the Internet of Things (IoT), where data is massive and constantly changing, the performance of IDS and IPS systems becomes more vulnerable to cyber threats. [42].

A major challenge in IDS and IPS deployment is the high rate of false positives, where benign activities are incorrectly flagged as malicious. This is particularly problematic in enterprise environments where false alarms can lead to unnecessary investigations and resource wastage. False positives can significantly reduce the effectiveness of these systems, as security teams may overlook legitimate threats due to alarm fatigue [43].

IDS and IPS systems require substantial computational resources, especially when deploying at the network perimeter or on high traffic networks. The processing power requires to inspect every packet and the memory needs to store large datasets can lead to significant performance degradation. In addition, for constraining resource environments such as IoT or edge computing, this becomes a major limitation [44].

Cyberattacks continually evolve their methods to bypass traditional IDS and IPS systems. Signature based detection systems, which rely on predefined attack signatures, are ineffective against unknown threat and zero-day attacks. Similarly, behavior-based systems which flag deviations from established network patterns, can struggle to differentiate between normal changes in behavior and actual attacks. The adaptability of IDS and IPS systems to new attack vectors remains a significant challenge [45].

The increase of cloud computing and virtualization technologies introduces additional complexities in IDS and IPS deployment. In cloud environments, the dynamic nature of virtual machines, shared resources, and multi-tenant architectures makes it challenging to monitor and protect against intrusions effectively. Traditional IDS/IPS systems that rely on static network configurations struggle to maintain visibility and control in such environments [46].

3.3 Strategy of improving IDS and IPS

The increasing sophistication of cyberattacks highlights the growing need for robust and adaptive intrusion detection systems (IDS) and intrusion prevention systems (IPS). IDS and IPS are essential in detecting and preventing unauthorized access and malicious activities within a network. However, existing systems face several challenges, including high false positive rates, inability to detect zero day or new attacks, and computational inefficiencies. To address these issues, recent advancements introduce AI techniques in improving detection accuracy, machine learning (ML) and deep learning (DL) into IDS and IPS design architecture [36], [49].

The evolution and methodologies of Anomaly-based Intrusion Detection Systems (IDS), highlighting their ability to detect unknown attacks by analyzing deviations from normal behavior. It emphasizes key challenges like false positives and data overload, and suggests future research should focus on hybrid techniques to enhance accuracy and reduce false detections [34], [37].

This study [12] discusses the integration of machine learning and deep learning techniques, such as decision trees (DT), support vector machine (SVM), convolutional neural network (CNN), and long short-term memory networks (LSTM) to enhance the accuracy and efficiency of IDS. The hybrid models aim to detect both known and unknown malicious threats, addressing the limitations of traditional rule- based IDS.
One unique insight is the proposal of a four-level security framework that combines anomaly and misuse-based detection with risk factor analysis to overcome limitations in existing IDPS models, it stresses the need for lightweight and resource efficient solutions tailored to the constraints of IoT devices and networks. Additionally, it highlights the potential of transfer learning to create adaptable and reusable intrusion detection models for dynamic IoT environments [27].

This article [48], provides a hybrid intrusion detection model merging neural networks and supporting vector machines to enhance detection accuracy. It indicates the limitations of signature based and anomaly-based IDS and IPS to present a solution that leverages the strengths of both approaches.

As the best method of reducing IDS and IPS in detecting and blocking the false positive detection and protection require to tune rules and regularly update signatures and threat intelligence feeds, by applying three components, including neighboring related alerts (NRA), analyses the temporal and spatial proximity of alerts to identify clusters indicative of true attacks, high alert frequency (HAF), and detects alerts that occur with high frequency, which often associate with misconfigurations and utilizes historical data to recognize alert patterns that identify as false positives detection [50].

By analyzing Snort and Suricata as IDS and IPS over four years period (2017-2020), focusing on updating signatures, and comparing past and future rule sets, it highlights the critical role for maintaining IDS and IPS in managing cyberthreats effectively [51].

4. Conclusion

In conclusion, the evolving nature of cyberthreats, especially, advanced persistent threat and zero-day threat, this research emphasizes the critical function of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in enhancing cybersecurity monitoring process in detecting and preventing cyberthreats in real time and automated response capabilities within organizational networks. In addition, it provides useful structure in implementing IDS and IPS for managing cyberthreats when integrating IDS and IPS properly. Furthermore, it discusses the benefits of using IDS and IPS, the challenge of using IDS and IPS, and strategy for improving IDS and IPS.

Key findings from this study consists of 4 main ideas.
First, combining network and host-based IDS and IPS technologies allow for both passive and active threat management, covering detection, analysis, and prevention to potential cyberthreats targeting the system.

Second, implementing next generation IDS and IPS by integrating with AI and machine learning can significantly improve the accuracy and responsiveness of intrusion handling in real time to reduce false positives and can detect and protect unknown threat.

Third, by reviewing configuration rules, continuous tuning, and regularly updating the latest signature and anomaly-based detection.

Fourth, by integrating IDS and IPS with threat intelligence from different sources as well as optimizing IDS and IPS to make sure it discovers the latest known and unknown threat effectively.

Although this research focuses primarily on IDS and IPS to help manage cybersecurity monitoring processes, its findings are applicable to broader digital information technology, including government, healthcare, financial, critical infrastructure, etc. As cyberattacks is persistent by incorporating intelligent intrusion systems will be useful in building resilient, scalable, and adaptable security operations across different sectors.

This research contributes for both conceptual and practical framework for implementing and optimizing IDS/IPS systems to improve cybersecurity monitoring process. It also offers guidance on combining detection and prevention capabilities with real time data analysis and threat intelligence to include this necessary evolution.

Despite the benefits, challenges, and strategy for improving IDS and IPS are reducing false positives, strengthening detection and prevention. Future research should explore AI and Machine learning adaptive IDS and IPS models, edge-based intrusion detection, and integration with autonomous response systems such as security information and event management (SIEM), and security orchestration, automation, and response (SOAR) to improve reliability in managing cybersecurity.

Corresponding author

Sokroeurn Ang
angsokroeurn.phdscholar@lincoln.edu.my

Acknowledgment

The authors thank their co-authors for guidance, peer reviewers for valuable feedback, and all participants for their contributions. They also acknowledge the support of the Lincoln University College Doctoral Program and appreciate the editorial team and anonymous reviewers of the Journal of Cyber Security and Risk Auditing for their constructive input.

Funding

This research received no external funding.

Contributions

S.A; M.H; S.H;M.J; Conceptualization, S.A; M.H; S.H;M.J; Investigation, S.A; M.H; S.H;M.J; A.A; Writing (Original Draft), S.A; M.H; S.H;M.J; and S.A; M.H; S.H;M.J; Writing (Review and Editing) Supervision, S.A; M.H; S.H;M.J; Project Administration.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Conflicts Of Interest

The author declares no conflicts of interest.

References

[1] Gupta, N., Jindal, V., & Bedi, P. (2023). A survey on intrusion detection and prevention systems. *SN Computer Science*, *4*(439), 1–5. https://doi.org/10.1007/s42979-023-01926-7

[2] Otoum, Y., & Nayak, A. (2021). AS-IDS: Anomaly and signature-based IDS for the Internet of Things. *Journal of Network and Systems Management*, *29*(3), 1–24. https://doi.org/10.1007/s10922-021-09589-6

[3] Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, *184*, 8–15. https://doi.org/10.1016/j.comnet.2020.107679

[4] Hawedi, M., Talhi, C., & Boucheneb, H. (2018). Multi-tenant intrusion detection system for public cloud (MTIDS). *Journal of Supercomputing*, *74*(12), 5201–5208. https://doi.org/10.1007/s11227-018-2572-6

[5] National Institute of Standards and Technology. (2007, February). *Guide to intrusion detection and prevention systems (IDPS)* (Special Publication 800-94). https://csrc.nist.gov/publications/detail/sp/800-94/final

[6] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *87*, 157–163. https://doi.org/10.1016/j.cose.2019.06.005

[7] Seo, W., & Pak, W. (2021). Real-time network intrusion prevention system based on hybrid machine learning. *IEEE Access*, *9*, 46387–46393. https://doi.org/10.1109/ACCESS.2021.3066620

[8] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *87*, 148–151. https://doi.org/10.1016/j.cose.2019.06.005

[9] Garcia, C. F. J., & Blandon, T. E. G. A. (2022). A deep learning-based intrusion detection and prevention system for detecting and preventing denial-of-service attacks. *IEEE Access*, *10*, 83044–83050. https://doi.org/10.1109/ACCESS.2022.319664

[10] Keegan, N., Ji, S.-Y., Chaudhary, A., Concolato, C., Yu, B., & Jeong, D. H. (2016). A survey of cloud-based network intrusion detection analysis. *Human-Centric Computing and Information Sciences*, *6*(19), 1–17. https://doi.org/10.1186/s13673-016-0076-z

[11] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), 1–9. https://doi.org/10.1002/ett.4150

[12] Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. *Journal of Cloud Computing, 13*(123), 6–18. https://doi.org/10.1186/s13677-024-00685-x

[13] Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors, 23*(5), 6–11. https://doi.org/10.3390/s23052415

[14] Issa, M. M., Aljanabi, M., & Muhialdeen, H. M. (2024). Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations. *Journal of Intelligent Systems, 33*(1), 15–26. https://doi.org/10.1515/jisys-2023-0248

[15] Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security, 102*, 7–17. https://doi.org/10.1016/j.cose.2022.102675

[16] Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Computers & Security, 114*, 540–550. https://doi.org/10.1016/j.cose.2022.102675

[17] Saito, S., Maruhashi, K., Takenaka, M., & Torii, S. (2016). TOPASE: Detection and prevention of brute force attacks with disciplined IPs from IDS logs. *Journal of Information Processing, 24*(4), 217–224. https://doi.org/10.2197/ipsjjip.24.217

[18] Aburomman, A. A., & Reaz, I. B. M. (2016). Review of IDS development methods in machine learning. *International Journal of Electrical and Computer Engineering (IJECE), 6*(6), 2432–2434. https://doi.org/10.11591/ijece.v6i6.12478

[19] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications, 36*(1), 48–53. https://doi.org/10.1016/j.jnca.2012.05.003

[20] Cañola Garcia, J. F., & Taborda Blandon, G. E. (2022). A deep learning-based intrusion detection and prevention system for detecting and preventing denial-of-service attacks. *IEEE Access, 10*, 83050–83055. https://doi.org/10.1109/ACCESS.2022.3196642

[21] Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences, 12*(21), 10–22. https://doi.org/10.3390/app122211752

[22] Thakkar, A., & Lohiya, R. (2022). A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review, 55*(4), 470–510. https://doi.org/10.1007/s10462-021-10037-9

[23] Kwon, H.-Y., Kim, T., & Lee, M.-K. (2022). Advanced intrusion detection combining signature-based and behavior-based detection methods. *Electronics, 11*(6), 2–4. https://doi.org/10.3390/electronics11060867

[24] Kikissagbe, B. R., & Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics, 13*(18), 1–2. https://doi.org/10.3390/electronics13183601

[25] Giri, A. L., & Annamalai, S. (2022). Intrusion detection system for local networks – A review study. In *Proceedings of the 2nd International Conference on Advances in Computing, Innovation and Technology in Engineering (ICACITE)* (pp. 1388–1391). https://doi.org/10.1109/ICACITE53722.2022.9823433

[26] Korčák, M., Lámer, J., & Jakab, F. (2014). Intrusion prevention/intrusion detection system (IPS/IDS) for WiFi networks. *International Journal of Computer Networks & Communications (IJCNC), 6*(4), 78–80. https://doi.org/10.5121/ijcnc.2014.6407

[27] Jayalaxmi, P. L. S. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T.-H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEE Access, 10*, 121185–121187. https://doi.org/10.1109/ACCESS.2022.3220622

[28] Chung, C.-J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). NICE: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE Transactions on Dependable and Secure Computing, 10*(4), 200–210. https://doi.org/10.1109/TDSC.2013.8

[29] Hart, M., Richardson, E., & Dave, R. (2024). The effects of IDS/IPS placement on big data systems in geo distributed wide area networks. *International Journal of Advanced Computer Science and Applications, 15*(9), 11–17. https://doi.org/10.14569/IJACSA.2024.0150902

[30] Ruíz-Lagunas, J. J., Antolino-Hernández, A., Torres-Millarez, C., Paniagua-Villagómez, O., Reyes-Gutiérrez, M. R., & Ferreira-Medina, H. (2019). How to improve the IoT security implementing IDS/IPS tool using Raspberry Pi 3B+. *International Journal of Advanced Computer Science and Applications, 10*(9), 399–402. https://doi.org/10.14569/IJACSA.2019.0100952

[31] Niksefat, S., Kaghazgaran, P., & Sadeghiyan, B. (2017). Privacy issues in intrusion detection systems: A taxonomy, survey, and future directions. *Computer Science Review, 25*, 70–73. https://doi.org/10.1016/j.cosrev.2017.07.001

[32] Seo, W., & Pak, W. (2021). Real-time network intrusion prevention system based on hybrid machine learning. *IEEE Access, 9*, 46386–46395. https://doi.org/10.1109/ACCESS.2021.3066620

[33] KKumar, S., Gupta, S., & Arora, S. (2021). Research trends in network-based intrusion detection systems: A review. *IEEE Access, 9*, 157761–157774. https://doi.org/10.1109/ACCESS.2021.3129775

[34] Samrin, R., & Vasumathi, D. (2017). Review on anomaly-based network intrusion detection system. In *2017 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT)* (pp. 142–145). https://doi.org/10.1109/ICEECCOT.2017.8284655

[35] Keegan, N., Ji, S.-Y., Chaudhary, A., Concolato, C., Yu, B., & Jeong, D. H. (2016). A survey of cloud-based network intrusion detection analysis. *Human-Centric Computing and Information Sciences, 6*(1), 2–14. https://doi.org/10.1186/s13673-016-0076-z

[36] Bedogni, L., Bousdekis, A., Von Stietencron, M., Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors, 23*(5), 2–13. https://doi.org/10.3390/s23052415

[37] Ho, C.-Y., Lai, Y.-C., Chen, I.-W., Wang, F.-Y., & Tai, W.-H. (2012). Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems. *IEEE Communications Magazine, 50*(3), 146–153. https://doi.org/10.1109/MCOM.2012.6163595
[38] Saito, S., Maruhashi, K., Takenaka, M., & Torii, S. (2016). TOPASE: Detection and prevention of brute force attacks with disciplined IPs from IDS logs. *Journal of Information Processing, 24*, 217–224. https://doi.org/10.2197/ipsjjip.24.217
[39] Sangaiah, A. K., Javadpour, A., & Pinto, P. (2023). Towards data security assessments using an IDS security model for cyber-physical smart cities. *Information Sciences, 617*, 2–13. https://doi.org/10.1016/j.ins.2023.119530
[40] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., Ahmad, F., & Khan, A. S. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 31*(10), 1–23. https://doi.org/10.1002/ett.4150
[41] Banu, N., & Sangeetha, S. K. B. K. B. (2025). Intrumer: A multi-module distributed explainable IDS/IPS for securing cloud environment. *Computers, Materials & Continua, 72*(1), 1–10. https://doi.org/10.32604/cmc.2024.059805
[42] Behravan, M., & Ghaffarian, S. (2019). A survey of intrusion detection and prevention systems. *Journal of Computer Networks and Communications, 2019*, 1–9. https://doi.org/10.1155/2019/5368421
[43] Yadav, S., & Saxena, M. (2020). Reducing false positives in intrusion detection systems using hybrid machine learning algorithms. *Future Generation Computer Systems, 107*, 107–115. https://doi.org/10.1016/j.future.2019.12.033
[44] Ahmad, A., & Khan, M. K. (2019). Machine learning-based IDS for reducing false positives in network security. *Computers & Security, 87*, 101557–101565. https://doi.org/10.1016/j.cose.2019.101557
[45] Wang, F., & Yao, L. (2020). A deep learning approach for intrusion detection system with reduced false positives. *Journal of Network and Computer Applications, 155*, 2–10. https://doi.org/10.1016/j.jnca.2020.102530
[46] Alsmadi, I., & Xu, D. (2015). Security of Software Defined Networks: A survey. *Computers & Security, 53*, 80–90. https://doi.org/10.1016/j.cose.2015.05.006
[47] Sharma, A., & Rani, A. (2018). Reducing false positives in intrusion detection systems using ensemble learning. *Journal of Computer Science and Technology, 33*(5), 1034–1040. https://doi.org/10.1007/s11390-018-1845-6
[48] Zhao, W., & Zhao, Z. (2024). Providing a hybrid approach to increase the accuracy of intrusion detection systems in computer networks. *Journal of Engineering and Applied Science, 71*, Article 123, 2–17. https://doi.org/10.1186/s44147-024-00404-y
[49] Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI-based intrusion detection system. *Measurement: Sensors, 28*, Article 100827, 2–10. https://doi.org/10.1016/j.measen.2023.100827
[50] Spathoulas, G. P., & Katsikas, S. K. (2010). Reducing false positives in intrusion detection systems. *Computers & Security, 29*(1), 36–40. https://doi.org/10.1016/j.cose.2009.07.008
[51] Asad, H., Adhikari, S., & Gashi, I. (2024). A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems. *International Journal of Information Security, 23*, 1332–1342. https://doi.org/10.1007/s10207-023-00794-9

Biographies

Author Sokroeurn Ang. Mr. Sokroeurn Ang is a senior lecturer in cybersecurity. He has been teaching ICT and cybersecurity since 2015 and has held various roles in ICT and cybersecurity for over a decade. His professional experience spans the central banking sector, private banking, and internet service providers. He has been actively involved in areas such as cybersecurity risk assessment, IT governance, network security, web application security, cybersecurity incident response, BCP and DRP, cloud security, VAPT, and IT auditing. Mr. Sokroeurn Ang completed a Micro-Master in Cybersecurity at the Rochester Institute of Technology (RIT), USA, and earned a Master's degree in Cybersecurity from Royal Holloway, University of London, UK. He is currently pursuing a PhD in Cybersecurity at the Lincoln University College, Malaysia. Mr. Sokroeurn Ang has been certified such as CISSP, CISA, CISM, CC, ECSA, CEH, CCNA Security, CCNA, CyberOps, and AWS Certified Cloud Practitioner. In addition, he is a certified Cisco Instructor and an AWS Academy Instructor. Email: angsokroeurn.phdscholar@lincoln.edu.my

Author Mony Ho. Mony Ho is a Ph.D. candidate in Information Technology at Lincoln University College, Malaysia. He holds a Master's degree in IT and Data Science from the European International University, France. He is currently a senior technical teacher at Preah Kossomak Polytechnic Institute and lectures part-time at multiple universities in Cambodia. His teaching and research interests include Data Science, Big Data, software engineering, cloud technologies, and web and mobile application development.

Author Sopheatra Huy. Sopheatra Huy is a Ph.D. candidate in Information Technology at Lincoln University College, Malaysia. He holds an M.Sc. in IT from the Royal University of Phnom Penh, Cambodia. With over a decade of experience as a part-time lecturer, he has taught programming, software engineering, and IT project management. Professionally, he is the Senior Manager of IT Audit at WB Finance and has previously worked with Phillip Bank and PRASAC MFI in similar roles. His research interests include IT automation, cybersecurity, and audit technologies.

Author Dr. Midhunchakkaravarthy Janarthanan. He is the Dean of the School of AI Computing and Multimedia at Lincoln University College, Malaysia. He holds a Ph.D. in Computer Science and has published extensively in the fields of Big Data, Web Text Mining, Machine Learning, and GPU Computing. With over 1,000 citations on Google Scholar, his research has made significant contributions to scalable data processing and intelligent computing. Dr. Midhunchakkaravarthy also serves as a research supervisor and mentor for numerous postgraduate students, supporting innovative work in artificial intelligence and cloud-based systems.