Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, No.2, March : 2025

ENHANCING CLOUD SECURITY THROUGH INTRUSION DETECTION AND PREVENTION MECHANISM WITH THE ASSISTANCE OF BIO-INSPIRED AND DEEP LEARNING TECHNIQUES: A SURVEY

Dr. K. Selvanayaki Research Supervisor Department of Computer Science VET Institute of Arts and Science Thindal, Erode.
Mrs. P. Gayathridevi Research Scholar Department of Computer Science VET Institute of Arts and Science Thindal, Erode

Abstract:
Intrusion Detection Systems (IDS) evaluates security incidents to alert users about threats but IPS protects systems actively during attacks in real time. This research analyzes the combination of bio-inspired together with deep learning approaches for improving processing power of Intrusion Detection and Prevention Systems (IDPS) in cloud environments. The distributed nature of cloud environments along with their dynamic resource-sharing mechanisms exposes them to security threats so robust intrusion prevention methods are imperative. Current standard IDPS methods face problems with many technical errors during threat detection and operate at insufficient speed while adjusting poorly to shifting attack styles. Bio-inspired algorithms that use nature-mimic process like swarm intelligence and genetic evolution develop adaptive intrusion detection systems with efficient detection performance. The joining of deep learning models with these hybrid approaches demonstrates outstanding capabilities for detecting complex patterns and anomalies across big datasets to address cloud security requirements. This survey examines and classifies different bio-inspired methods such as ant colony optimization and artificial immune systems together with deep learning architectures featuring recurrent neural networks (RNNs) and convolutional neural networks (CNNs). The survey analyzes how effectively these methods detect modern cyber threats and how they stop zero-day exploits and enhance their detection performance. The discussion includes important evaluation criteria along with limitations that influence practical implementation of these methods in this field. The research investigates bio-inspired alongside deep learning-driven IDPS frameworks which serve as intelligent security solutions for modern cloud computing environments.

Keywords:

Introduction

In modern society, the internet-based services are getting too much popularity from last few decads. In today's world, people typically use smartphones, laptops, tablets and other gadgets to access these services at any time, from anywhere. Therefore, data that streams via these networks may contain essential or sensitive information. Moreover, due to advancement of internet technology, the sensitive data is always transmitted between devices and data-warehouse for storing and retrieval purpose. These results open trapdoor for the attackers to launch the widespread of attacks that may be threatened to the organisation and/or the individuals. Attackers use a variety of cutting-edge approaches to take advantage of system security flaws. This might result in the misuse of confidential or delicate information, unauthorised access to the system, or a breach of client accounts. Security professionals and system administrators must employ the advanced security techniques to defend against these threats. Additionally, as new technologies developed for instance big data, IoTs, etc., the vast volumes of traffic or data are also growing, gradually. Therefore, updating the attack signature is getting harder, slower, and more tedious because of the network data traffic expanding significantly.

Moreover, searching through such large amounts of data in hunt of relevant or useful evidence is a critical task for data scientists, commercial corporations, and marketers. Hence, network security is presently a rising field of study for scientists and academics because of increased traffic and extensive internet usage. Researchers in these fields (network security) attempt to prevent intrusions or attackers

from exploiting system or network vulnerabilities to gain unauthorised entry (s). Although many prevention technologies such as Antivirus, firewalls, etc., for securing a network or system have been developed since last two decades to detect and eliminate potential attacks such as DoS, user to root (U2R), remote to local (R2L), Probe, etc. As a result, fundamental security procedures are needed to identify new kinds of attacks as well as unwanted traffic or data that could harm or disrupt a particular host or network. Among many, one of the prominent security techniques used to safeguard the network or system is an IDS [1]. An IDS is a collection of hardware and/or software tools that can gather, analyse, and identify incoming traffic to spot potential threats, masquerade [2] attacks (in which an unauthorised user impersonates a valid user to access that user's data), and unwanted traffic in networks, and particular systems.

The IDS also protects sensitive data from unauthorised access while it is being sent over networks. To achieve these capabilities and goals, IDS should be investigated and understood the information obtained using specific mathematical or statistical approaches, and it should also alert any network administrators of suspicious activities [3]. The three types of IDS techniques based on detection approaches, namely signature-based IDS, specification-based IDS, and anomaly-based IDS [4]. IDS is constantly vulnerable to hidden attacks [5] and a variety of potential threats, even though numerous IDS have been developed over the last two decades to detect and protect potential attacks, they still lack sufficient flexibility and scalability. Yahoo revealed two data breaches between 2014 and 2016 that affected 500 million customers‟ accounts and cost the company 350 million dollars [6]. With the use of clever and advanced algorithms, the outbreaks are being pounded with the goal of snipping data. A zone of IDS continues to be dynamic for the researchers as attacks (outbreaks) rise as everything else does [7].

A robust IDS is necessary to analyse the massive data, extracts the significant features, identify and categorise the traffic as a normal or assaults. However, to analyse incoming traffic, it might be challenging for IDS to extract useful or pertinent information from the massive amounts of data generated by evolving technologies and transmitted over networks. To address these challenges, IDS must employ a large dataset and a FST capable of eliminating out irrelevant data and identifying the features that impact to attack detection. Moreover, a large dataset sometimes contains noise as well as redundant or duplicate elements. In addition, possible side effect of considering a massive dataset is that the feature count rises in direct correlation with the total number of observations. This may lead to a significant number of false-positive (FP) findings. Although numerous features in IDS datasets provide a light on traffic flow anomalies, but not all of them may be necessary for detection. Therefore, picking more useful features can boost IDS efficiency and effectiveness.

Many studies have used optimization techniques in this context to address data dimension issues and boost the efficiency of IDS in the literature. Based on the evaluation criterion, optimization techniques are separated into three categories: filter, wrapper, and hybrid techniques [8]. In which wrappers, are objective functions that use training models to exploit a subset of features before adding or removing features based on the prior model. Whereas filters are objective functions that evaluate the information content of data based on data attributes (e.g., inter-class distance, correlation measures) And, finally Hybrid; these strategies combine the advantages of the prior techniques at various points in the selecting process. However, at many situations, its may be always impossible to obtain the best subset of features using filter-based techniques, but wrapper-based techniques can always produce excellent results.

In this research, wrapper-based optimization techniques have used, as it is more accurate than filter-based optimization techniques and can be adapted to the classifiers [9]. This wrapper-based method employs the classification algorithm to evaluate a subset of features. These techniques examine features and extract the best subsets based on feedback from learning algorithms (such as classifiers), and they frequently outperform filter-based techniques in terms of accuracy [10]. When employing a wrapper-based optimization techniques, three main factors must be considered [11]: the classifier, the standards for evaluating the subset of features (accuracy, Precision, etc.), and the search techniques

used to find the best feature hybridization [12]. In applications like IDS, where detection accuracy is most important; wrapper-based feature selection is preferable. To improve efficiency while reducing computation complexity, some researchers have created hybrid optimization techniques that mix wrapper and filter approaches [13-17].

Due to the advancement of Internet technology, the Internet based services are getting trendy from last two decades, especially after Covid-19 pandemic. People typically use smartphones, laptops, tablets, and other electronics gadgets to get access such services at any time and from any location. As a result, the data start traveling through these networks between the machines and data storage centres that could contain sensitive or private information. Hence, it also creates a new opportunity for the attackers to break the security walls and launch the widespread of attacks that may be threatened to the organisation and/or the individuals. Attackers use a variety of cutting-edge tactics to attack system security flaws. This might result in the misuse of private or sensitive information, unauthorised access to the system, or a breach of client accounts. To defend against these assaults, safeguard highly sensitive data and protect the networks from any external threats is become primary concern for the researchers and scientist.

One of the most prominent and popular mechanism is IDS which investigate incoming traffics and classified either as a legitimate or malicious in order to detect potential threats or to spot suspicious activity in specific systems or networks. However, a significant amount of network traffic is generated and exchanged in the network in every interval because of the spread of ubiquitous technologies like the internet, social media, IoTs, etc. Moreover, the features produced by network traffic may include several unimportant or noisy attributes. In order to adequately solve this issue, some lightweight detection methods and feature selection or elimination approaches must be implemented in IDS, to avoid the higher system's processing time and computational cost. As a result, decision engines and feature reduction or elimination models should be created with a lightweight characteristic [17]. Further, using a single classifier or estimator for model evaluation and comparison may be a bad choice. It would be beneficial to compare the prediction accuracy of several classifiers [18].

Intrusion Detection and Prevention System

Encryption, secure network protocols, and firewalls are just a few of the techniques and technologies that have been used to restrict unauthorized use of computer systems. As security technologies advance, hackers also keep implementing fresh methods for compromising the security of computer systems. In addition to the constantly evolving assault methods, new network kinds like wireless sensor network, software defined networks, etc., have emerged, making it more difficult to ensure the security of computer systems. These contemporary network kinds are not created with security in mind. The majority of conventional security techniques are unable to offer adequate security over these networks. A security system that can identify any illegal attempts to access a computer system is therefore urgently needed. As a result, the IDS created and is now regarded as a crucial component of security systems. An IDS is a method of examining and tracking activity within a computer or network system in order to detect possible threats or intrusion by assessing violations of computer security principles: confidentiality, integrity, and authentication (CIA) [19]. Intrusion detection process consists of following steps [20]:

- Monitoring network traffic.
- Collecting data from network packets.
- Processing data for analysis.
- Identifying signatures and deriving patterns.
- Comparing patterns with the stored signatures and/or patterns.
- Generating alarm if any unusual behavior or pattern is recognized

IDSs can be used in combination with other security tools like firewalls and access controls, among others. Along with IDS, these security measures examine the data and protect the network from abnormalities. An IDS installed in a network looks at network activity in order to learn about possible

threats and weaknesses that could harm the system and the network environment. An IDS also attempts to show verifiable evidence of intrusions into information systems. It main goal is to quickly and accurately identify all breaches. It seeks to deliver reliable evidence of information systems being breached. By using IDS, network administrators can identify security goal violations. Security objective breaches can range from outside intruders trying to disable resources or compromise network security architecture to internal users abusing their access to system resources. The effective and efficient development of IDS, however, is a real challenge due to the requirement of a high true positive rate and low false positive rate for the constantly changing pattern of intrusions while using the least amount of computing resources as quickly as feasible. The quick detection of a breach may reduce the damage caused by unauthorized access to a computer system. The first version of IDS was put forth by Denning [21]. Figure 1 depicts its detection and response process. This proposed model [22] of IDS are developed and described to handle the issues of intrusion happening both internally and externally to the network.

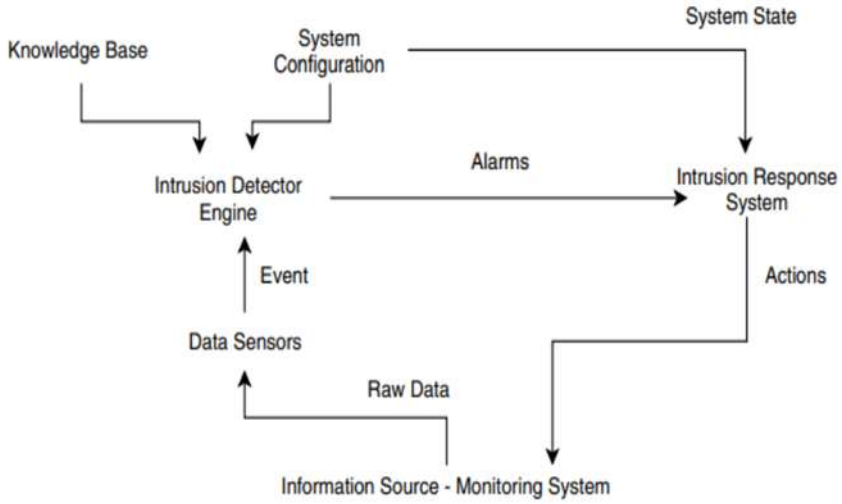

Figure 1. Intrusion detection and response technique.

The presented model is made up of a component called a knowledge base, which serves as the foundation for statistical operations on data collected from sensors placed throughout the environment. The knowledge base includes individual profile data, configuration information for host and target systems, and information on attack patterns and signatures. However, a rule-based strategy is also put forth to identify intrusions and unusual behavior by flagging patterns identified through research into the activities of legitimate users [23]. The application of a rule-based approach is founded on the network and system's prior knowledge [24].

As previously stated, an IDS tries to monitor a network or particular system by detecting malicious actions in a timely way. In [25] present an IDS's taxonomy based on four major distinct dimensions: data source, system distribution, detection strategy, and timeliness. To recapitulate, in summary, Figure 2. demonstrates the range of IDSs covered in [25].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, No.2, March : 2025

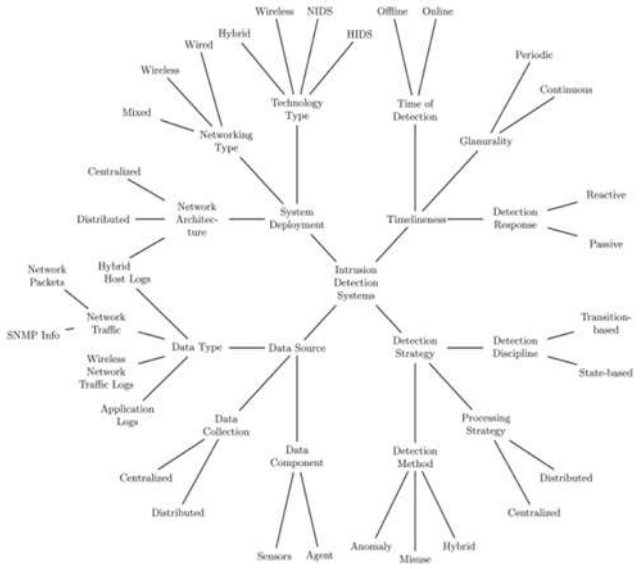

Figure 2. IDS‟s taxonomy

An IPS functions as a network security device which monitors networks shouldering the role of spotting attacks then blocking unwanted intrusions before they can occur. An essential network defense technology protects systems through immediate adversarial threat reactions which derive from analyzing network traffic patterns to detect suspicious behavior. Unlike IDS which identifies threats then sends alerts to administrators an IPS performs real-time threat prevention and mitigation to lower the risk of damage.

IPS warns about and defends against threats through multiple detection methods. Signature-based detection technology matches incoming network data with stored attack signatures to find malicious activities within its reference library. While the signature-based detection method stops known documented threats it fails to detect newly emerging or unknown attacks efficiently. The problematic limitation gets addressed through machine learning models from anomaly-based detection which enable traffic baseline pattern creation for detecting abnormal activities that might show signs of attack. The deterrence of zero-day vulnerabilities together with complex threats exists within this detection approach. Security policies established by administrators are enforced using policy-based detection methods which combine with behavior-based detection to analyze network patterns for detection of suspicious activities.

The deployment method and operational parameters divide IPS solutions into distinct categories. When installed strategically throughout the network a NIPS system monitors and defends all network activities. HIPS provides gateway-like protection as an installed program on each endpoint through endpoint monitoring of system calls and file access and application activities. WIPS protects wireless networks through detection of unauthorized access points along with potential rogue devices within the network. With Content-Based IPS technology (CIPS) operators inspect network traffic content throughout HTTP or email communications to stop attacks based on specific content.

The primary functions of an IPS include traffic monitoring, threat detection, policy enforcement, and threat mitigation. A system detects potential threats by automatically initiating response actions including packet drops and connection resets along with firewall rule adjustments to stop additional attacks. The proactive nature of IPS makes it an essential system for protecting information assets while assuring the integrity of important operational facilities [26].

Network security improvements are one of the main uses of IPS throughout different operational situations. Network resources stay protected against distributed denial-of-service (DDoS) attacks because this technology serves as a critical preventive measure. The security system successfully stops vulnerabilities that target web applications including SQL injection and cross-site scripting (XSS). IPS serves two major defense functions: it detects unreported zero-day vulnerabilities through its capability

to identify unique attack patterns while it maintains visibility on internal network behavior to defend against malicious insiders.

An IPS functions within modern cybersecurity structures alongside firewall systems and both antivirus solutions and security information and event management (SIEM) tools. Through multiple layers security systems achieve complete protection against present-day and future cyber threats. The rising adoption of cloud-based plus hybrid network systems has elevated the critical nature of IPS systems to establish secure resilient operations. Artificial intelligence and machine learning exists as a core element of IPS to support stronger threat detection precision as well as adaptive responses throughout complex network scenarios [27].

Comprehensive Analysis of IDS and IPS

The development of effective Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) has become a crucial area of research in enhancing cybersecurity across diverse domains. As the complexity and volume of cyber threats continue to rise, innovative techniques such as machine learning (ML), deep learning (DL), and hybrid models have been employed to improve the detection, prevention, and mitigation of attacks. This paper presents a comprehensive analysis of recent advancements in IDS and IPS. Tables 1 and 2 summarize the key techniques, evaluation datasets, and references of prominent studies, highlighting the evolving trends and solutions proposed by researchers to address specific cybersecurity challenges.

Table 1. Comprehensive Analysis of Intrusion Detection System

Focus Area	Key Technique	Evaluation Dataset	Reference	Inference & Description
IDS for In-Vehicle Networks (IVNs)	ML, DL, and Hybrid Models	CAN Protocol	[1]	The paper categorizes IDS techniques for IVNs and emphasizes transitioning from signature-based to anomaly-based detection. ML and DL approaches show significant improvements in detecting spoofing and denial-of-service attacks in IVNs.
Botnet Detection in IIoT	25+ ML Algorithms	IoT Dataset	[2]	This study benchmarks over 25 ML models for botnet detection across seven IoT devices. The findings highlight that certain models achieve near-perfect accuracy, while others require dataset-specific optimization.
Distributed IDS Framework	Federated Learning	Decentralized Data	[3]	Federated Learning (FL) ensures privacy-preserving IDS by enabling collaborative model training on distributed data. The paper evaluates various aggregation strategies, emphasizing privacy-preserving techniques and decentralized security.

Cyber Threat Detection	SVM with PSO	Not Mentioned	[4]	This research integrates SVM with feature selection and optimization techniques like PSO to enhance intrusion detection accuracy. The model demonstrates superior classification performance with reduced computational complexity.
Complex Network Traffic	CNN-Focal Model	Open Network Dataset	[5]	By leveraging CNN and SoftMax classification, the proposed CNN-Focal model improves abnormal traffic detection accuracy. Experimental results show promising detection performance in complex network environments.
IoT Device Security	XGBoosting Classifier	IoT-NI Dataset	[6]	The study proposes an ensemble-based IDS using XGBoosting for smart home devices. The model efficiently detects nine types of attacks with high precision, demonstrating its effectiveness in IoT security.
Attack Classification	DCRNN with IGOA	UNSW-NB-15, CICDDoS2019, CIC-IDS-2017	[7]	This work introduces a DCRNN model optimized by IGOA for detecting network attacks. Feature selection using NBGOA significantly reduces data complexity, leading to improved classification accuracy and processing time.
Intrusion Detection Optimization	DL with Clustering & Optimization	CICIoT2023	[8]	The paper addresses high dimensionality challenges in intrusion datasets by proposing a clustering technique combined with optimization algorithms. Results demonstrate improved detection rates compared to previous models.
Protocol Standardization	Modified J48 Algorithm	Custom Protocol Data	[9]	This research focuses on standardizing protocol structures and using genetic algorithms for intrusion detection. The modified J48 algorithm outperforms traditional methods in attack detection efficiency.

Intrusion Classification	M-MultiSVM Model with ONgO	CSE-CIC-IDS 2018, UNSW-NB15	[10]	The study proposes a hybrid M-MultiSVM model with ONgO for efficient intrusion detection. Results show 99.89% and 97.53% accuracy on two datasets, demonstrating its robustness in attack detection.

Table 2. Comprehensive Analysis of Intrusion Prevention System

Focus Area	Key Technique	Evaluation Dataset	Reference	Inference & Description
Secure In-Vehicle Communication	Blockchain with IDS	CAN Dataset	[11]	This research explores the integration of blockchain for secure in-vehicle communication in IDS. It emphasizes distributed ledger technology to enhance data integrity and mitigate cyber threats in IVNs.
Industrial IoT Security	Federated Learning (FL)	IoT-23 Dataset	[12]	FL-based IDS is proposed to secure industrial IoT environments. The study demonstrates enhanced intrusion detection performance while preserving data privacy through decentralized learning mechanisms.
Attack Detection & Mitigation	Hybrid ML-DL Model	UNSW-NB15	[13]	The paper presents a hybrid ML-DL approach for detecting sophisticated cyberattacks. The hybrid model significantly improves detection accuracy and reduces false alarm rates in IDS.
Distributed IDS for Smart Cities	Edge-based IDS	IoT-NI Dataset	[14]	This research proposes an edge-based IDS architecture for smart cities, aiming to reduce latency and improve real-time intrusion detection. The approach enhances security in IoT systems by processing data at the edge.
Lightweight IDS for IIoT	Lightweight CNN	Industrial IoT Dataset	[15]	A lightweight CNN model for IDS is designed to operate in IIoT environments with limited computational resources. The study demonstrates the model's

				efficiency in detecting attacks with minimal overhead.
IDS for Cloud Computing	Hybrid Ensemble Model	Cloud Dataset	[16]	This paper proposes a hybrid ensemble model combining multiple ML algorithms to enhance IDS in cloud computing. It shows improved scalability and robustness in detecting cloud-specific threats.
Privacy-Preserving IDS for IoT	Homomorphic Encryption	IoT Dataset	[17]	The paper introduces a privacy-preserving IDS using homomorphic encryption for secure data processing in IoT systems. It addresses the challenge of maintaining privacy while ensuring accurate attack detection.
Cyber Threats in Smart Grids	DL-based IDS	Smart Grid Dataset	[18]	The research applies deep learning techniques to IDS for smart grid security, highlighting the importance of anomaly detection to prevent cyber-attacks in critical infrastructure systems.
IoT Device Security	Reinforcement Learning	IoT Device Dataset	[19]	This study utilizes reinforcement learning for IDS in IoT devices. It emphasizes continuous learning and adaption to new attack patterns, providing dynamic and resilient security for IoT environments.
Anomaly-Based IDS for Mobile Networks	Anomaly Detection with Autoencoders	Mobile Network Dataset	[20]	The paper proposes an anomaly-based IDS using autoencoders to detect unusual patterns in mobile network traffic. The approach is effective in identifying novel cyber threats while minimizing false positives.

Conclusion

The survey highlights how bio-inspired and deep learning approaches strengthen cloud security by developing innovative Intrusion Detection and Prevention Systems (IDPS). Traditional security solutions lack the necessary capabilities to protect cloud environments from modern sophisticated cyber threats which continue to develop and intensify. Biological inspired optimization techniques based on ant colony optimization along with genetic algorithms produce flexible security solutions that model natural evolutionary processes. Deep learning models consisting of convolutional and

recurrent neural networks achieve premier results by tracking complex cyber-attacks while reducing misidentification rates. Multiple detection strategies together create an optimistic foundation for building smart proactive IDPS systems. To achieve practical implementation researchers need to tackle challenges that include complex computation along with model interpretability and real-time processing requirements. The path forward should involve model optimization of hybrid systems and deployment of federated learning technology to match security needs of decentralized networks and create efficient energy management frameworks for deep learning frameworks. The future development will lead to improved cloud security solutions that provide greater scalability alongside stronger adaptability for ever-changing computing environments.

Hybrid Intrusion Detection and Prevention Systems (IDPS) need focused research to create lightweight scalable solutions which integrate bio-inspired and deep learning techniques into cloud environments. Three main problems exist in building robust intrusion detection systems: achieving maximum speed in computation while maintaining simple training procedures alongside real-time security alert generation capabilities. Federated learning represents an optimistic development direction because it supplies decentralized security protection without sacrificing data privacy measures while XAI brings clarity to models to enhance transparency. The development of energy-conserving security algorithms combined with flexible adaptive procedures designed to function within changing threat environments will produce superior resilient cloud security solutions.

References

1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), e4150.
2. Almehdhar, M., Albaseer, A., Khan, M. A., Abdallah, M., Menouar, H., Al-Kuwari, S., & Al-Fuqaha, A. (2024). Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. *IEEE Open Journal of Vehicular Technology*.
3. Amru, M., Kannan, R. J., Ganesh, E. N., Muthu marilakshmi, S., Padmanaban, K., Jeyapriya, J., & Murugan, S. (2024). Network intrusion detection system by applying ensemble model for smart home. *International Journal of Electrical & Computer Engineering (2088-8708)*, *14*(3).
4. Aulia, A. R., Alwi, E. I., & Gaffar, A. W. M. (2024). Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables. *LINIER: Literatur Informatika dan Komputer*, *1*(3), 235-240.
5. Gheni, H. Q., & Al-Yaseen, W. L. (2024). Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset. *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, *9*, 100673.
6. Goswami, A., Patel, R., Mavani, C., & Mistry, H. K. (2024). Intrusion Detection and Prevention for Cloud Security. *International Journal on Recent and Innovation Trends in Computing and Communication*, *12*(2), 556-63.
7. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, *26*(6), 3753-3780.
8. Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, *10*, 100053.
9. Jaber, A. (2024, April). Transforming Cybersecurity Dynamics: Enhanced Self-Play Reinforcement Learning in Intrusion Detection and Prevention System. In *2024 IEEE International Systems Conference (SysCon)* (pp. 1-8). IEEE.
10. Khan, M. A. R., Shavkatovich, S. N., Nagpal, B., Kumar, A., Haq, M. A., Tharini, V. J., ... & Alazzam, M. B. (2022). Optimizing hybrid metaheuristic algorithm with cluster head to improve performance metrics on the IoT. *Theoretical Computer Science*, *927*, 87-97.

11. Khraisat, A., Alazab, A., Singh, S., Jan, T., & Jr. Gomez, A. (2024). Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions. *ACM Computing Surveys*, *57*(1), 1-38.
12. Kizza, J. M. (2024). System intrusion detection and prevention. In *Guide to computer network security* (pp. 295-323). Cham: Springer International Publishing.
13. Kudin, A., Grigorieva, O., & Nosok, S. (2024). The methods of decreasing FP in Anomaly based Intrusion Prevent System by using of complex information about information system. *Theoretical and Applied Cybersecurity*, *6*(1).
14. Kumar, G. S. C., Kumar, R. K., Kumar, K. P. V., Sai, N. R., & Brahmaiah, M. (2024). Deep residual convolutional neural network: an efficient technique for intrusion detection system. *Expert Systems with Applications*, *238*, 121912.
15. Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE Access*, *9*, 101574-101599.
16. Lee, A. Y. P., Wang, M. I. C., Hung, C. H., & Wen, C. H. P. (2024). PS-IPS: Deploying Intrusion Prevention System with machine learning on programmable switch. *Future Generation Computer Systems*, *152*, 333-342.
17. Lin, P. S., Lai, Y. C., Liao, M. L., Chiu, S. P., & Chen, J. L. (2024, February). Hybrid Clustering Mechanisms for High-Efficiency Intrusion Prevention. In *2024 26th International Conference on Advanced Communications Technology (ICACT)* (pp. 01-06). IEEE.
18. Nidamanuri, N. D. S. (2024). AI techniques applied to network intrusion detection system by using genetic approaches.
19. Ohri, P., Arockiam, D., Neogi, S. G., & Muttoo, S. K. (2024, February). Intrusion Detection and Prevention System for Early Detection and Mitigation of DDoS Attacks in SDN Environment. In *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)* (pp. 1-6). IEEE.
20. Rahul, Mukherjee, R., & Shekar, N. (2024, February). ML-Powered Intrusion Prevention for XSS Defense in Web Apps. In *International Conference On Innovative Computing And Communication* (pp. 343-351). Singapore: Springer Nature Singapore.
21. Selvan, M. A. (2024). SVM-Enhanced Intrusion Detection System for Effective Cyber Attack Identification and Mitigation.
22. Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. *Advanced Engineering Informatics*, *62*, 102685.
23. Singh, V. K., Sivashankar, D., Kundan, K., & Kumari, S. (2024). An Efficient Intrusion Detection and Prevention System for DDOS Attack in WSN Using SS-LSACNN and TCSLR. *Journal of Cyber Security and Mobility*, 135-160.
24. 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*(1), 453-563.
25. Tharini, V. J. (2024). Cross-Entropy Assisted Optimization Technique for High Utility Itemset Mining from the Transactional Database. *Communications on Applied Nonlinear Analysis*, *31*(3s), 90-104.
26. Turukmane, A. V., & Devendiran, R. (2024). M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning. *Computers & Security*, *137*, 103587.
27. Zhao, F., Li, H., Niu, K., Shi, J., & Song, R. (2024). Application of deep learning-based intrusion detection system (IDS) in network anomaly traffic detection. *Appl. Comput. Eng*, *86*, 231-237.