IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 10, October 2024

DOI: 10.17148/IJARCCE.2024.131019

A Survey: Intrusion Detection and Prevention System Using Machine Learning and Deep Learning Techniques

Prathamesh Margale[1], Shreya Kadam[2], Atharva Kakade[3], Prasad Papade[4] and

Prof. Naved Raza Q. Ali[5], Prof. Ganesh D. Jadhav[6]

Undergraduate Research Paper, Department of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India[1 ,2, 3, 4]

Department of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India[5 ,6]

Abstract: In the face of rapidly advancing cybersecurity threats, Intrusion Detection and Prevention System (IDPS) have established themselves as critical tools for warding off harmful activities against a network. Based on this consideration, this review tracks the development and impact of Machine Learning and Deep Learning strategies as associated with IDPS, focusing particularly on their ability to enhance detection performance. We have Surveyed various Intrusion Detection and Prevention System Datasets for assessing their effectiveness in detecting network intrusions. More importantly, it focuses on critical datasets and talks about the pros associated with them, such as better detection capability and their flexibility toward ever-evolving threats, but failed to fight some limitations like increased computational complexity and complex real-time traffic management. This survey gives an overview of the evolution and effectiveness of "Machine Learning and Deep Learning" techniques in advancing IDPS, addressing major concerns over issues of scalability, false positive rates, accuracy, Recall, Precision, F1 Score and overall system efficiency, with an aim to improve the fairness and reliability of intrusion detection and prevention system mechanisms.

Keywords: Intrusion Detection and Prevention System, Machine Learning, Deep Learning, Network Security, Random Forest, Support Vector Machine, Convolutional Neural Networks, Cybersecurity, Anomaly Detection, False Positives, Real-time Traffic, Scalability, Detection Accuracy.

I. INTRODUCTION

Rapid development of computer networks, spreading IoT devices, and huge range of related applications in the modern cybersecurity landscape have posed the issue of cybersecurity in a critical way. This is because of the relentless growth of cyber threats while it expands the necessity to ensure secure computer systems and sensitive data within governmental, commercial, and other sectors. The role of Intrusion Detection and Prevention Systems (IDPS) is very crucial in network security, which guards this information from a host of threats, intrusions, and malicious activities.

An IDPS operates by monitoring the network traffic and system activities for intrusion signs, including unusual traffic patterns, known malware signatures, or exploitation attempts of software vulnerabilities. IDS are primarily responsible for intrusion detection. They alert security personnel in case of any potential intrusions. However, an IPS actively prevents unauthorized access and malicious actions. Despite this, traditional IDPS approaches face challenges in accurately identifying intrusions, managing large data volumes, and filtering out false alarms amidst the growing complexity of cyber-attacks. These challenges have created a strong demand for integrating Machine Learning and Deep Learning techniques into IDPS, which offer promising avenues for improving network protection and enhancing the overall effectiveness of cybersecurity defences.

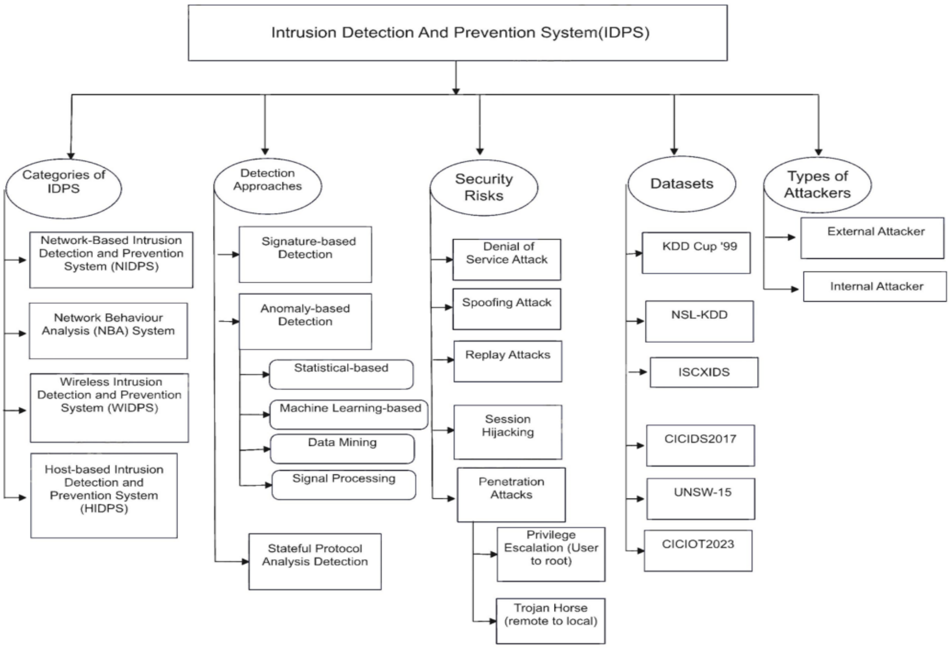
Intrusion Detection And Prevention System(IDPS)
Categories of IDPS
Network-Based Intrusion Detection and Prevention System (NIDPS)
Network Behaviour Analysis (NBA) System
Wireless Intrusion Detection and Prevention System (WIDPS)
Host-based Intrusion Detection and Prevention System (HIDPS)
Detection Approaches
Signature-based Detection
Anomaly-based Detection
Statistical-based
Machine Learning-based
Data Mining
Signal Processing
Stateful Protocol Analysis Detection
Security Risks
Denial of Service Attack
Spoofing Attack
Replay Attacks
Session Hijacking
Penetration Attacks
Privilege Escalation (User to root)
Trojan Horse (remote to local)
Datasets
KDD Cup '99
NSL-KDD
ISCXIDS
CICIDS2017
UNSW-15
CICIOT2023
Types of Attackers
External Attacker
Internal Attacker

Fig. 1 Intrusion Detection and Prevention System

Categories of IDPS: IDPS are categorized in four different types based on their operational scope within the network.

Network-based Intrusion Detection and Prevention System (NIDPS): A network-based Intrusion Detection and Prevention System monitors and analyses network traffic in the detection of intrusions that may impact the network infrastructure. This one is highly effective for detecting threats across an extensive network when analyzing patterns of traffic flow. This system passes through data packets and, yes, can identify suspicious activity at the perimeter level. NIDPS often comes integrated into firewalls and other related tools in network security, offering all-rounded protection.

Network Behaviour Analysis (NBA) System: NBA system is concerned with the identification of atypical patterns or behaviours in network traffic that may signify intrusions or malicious activities. It places significant emphasis on anomaly detection by examining deviations from standard network behaviour.

Wireless Intrusion Detection and Prevention System (WIDPS): WIDPS systems ensure there are no unauthorized access attempts or threats that are specific to wireless communications. Such a system is therefore crucial security over Wi-Fi networks, as it detects rogue access points and suspicious wireless activity, such as threats specific to wireless protocols, like eavesdropping and spoofing. WIDPS can also be useful in enforcing security policies for mobile and remote access points.

Host-based Intrusion Detection and Prevention System (HIDPS): HIDS functions at the host or device level to detect threats that are host-local, including unauthorized access and modification of files, for example. This system is meant to protect and safeguard individual machines from inside and outside threats through system-level activities monitoring.

Detection Approaches: These are the methods or techniques by which an IDPS can detect hostile activity.

Signature-based Detection: This is the technique that relies on known patterns of attack signatures to detect threats. Here, it matches observed behaviour against a database of known attack signatures and those same patterns fit to detect intrusions.

Anomaly-based Detection: It focuses on detects unusual activities or deviations from well-learned norms of behaviour. This methodology is actually beneficial in detecting new or unidentified threats through emphasis on anomalies. Anomaly-based detection has the capability to adjust dynamically according to changes made in network behaviour, making it ideal for environments where patterns vary through time. However, it may return more false positives than signature-based detection does because not all anomalies are malicious by nature.

Statistical-based Detection: Uses statistical techniques to analyze data for anomalous patterns, largely used within anomaly-based detections to detect anomalous statistical patterns.

Machine Learning-based Detection: Uses machine learning algorithms to learn normal behaviours and detect anomalies, with continually increasing precision over time.

DOI: 10.17148/IJARCCE.2024.131019

Data Mining: Uses data mining techniques for finding patterns in large amounts of data, usually utilized in intrusion detection to look for trends.

Signal Processing: It would process the network traffic signal to extract useful features for detection.

Stateful Protocol Analysis Detection: This entails monitoring the protocol state and behaviour with the aim of discovering anomalous behaviour. This technique compares the observed protocol behaviour to standards established, through which deviations may be detected as being relevant to malicious actions.

Security Risks: Lists common types of security threats IDPS aims at detecting and preventing, hence posing a serious threat in network security

Denial of Service Attack (DoS): An attacker saturates the system, server, or application with a deluge of requests, slowing it down, crashing it, or rendering it ineffective for legitimate users. DoS attacks interfere with resource availability.

Spoofing Attack: In a spoofing attack, the attacker impersonates a trustworthy entity by falsifying data-such as IP addresses or emails-to gain unauthorized access, intercept sensitive data, or redirect traffic to malicious sites.

Replay Attacks: Replay involves capturing and resending valid data transmissions to inoculate the system through misrepresentation or acceptance of the actions as being the same; this may lead to unauthorized access or ongoing fraudulent activity.

Session Hijacking: An attacker seizes an active session of the user, often by stealing a session token; this allows impersonation of the user and provides access to sensitive information or the ability to carry out unauthorized actions.

Penetration Attacks: Involves attempts to gain unauthorized access by exploiting vulnerabilities in systems.

Privilege Escalation (user to root): The attacker elevates their privileges from lower-level to root level or administrator level, facilitating the action of sensitive commands and access to restricted data.

Trojan Horse (Remote to Local): In this form of attack, a malicious program disguises itself as a normal application and thus permitting remote attackers to obtain local access and perform destructive actions on the compromised machine.

Datasets: Lists prominent datasets used in IDPS research for testing and validating detection techniques. These datasets provide structured data for assessing the effectiveness of various detection algorithms.

KDD Cup 99: It is a prominent dataset used in intrusion detection research, focusing on classical network attacks such as Denial of Service (DoS), User-to-Root (U2R), Root-to-Local (R2L), and Probe attacks. However, this dataset has class imbalance and repeated records.

NSL-KDD: This dataset is a refinement that compensates for these problems by balancing the class distribution and removing those redundant instances and thus is more suitable for research. The structure of the features is common to both datasets.

ISCXIDS: The Canadian Cyber Security Incident Response Centre designed the ISCXIDS dataset. It profiles a different range of attacks compared to the other two datasets. This dataset comprises web attacks, botnets, and reconnaissance so that it more closely resembles the modern threats relevant to the network.

CICIDS 2017: It is the updated version of ISCXIDS, which was also developed by the Canadian Cyber Security Incident Response Centre, CCIRC. The ISCXIDS framework is further improved in order to add more attacks, including HTTP and HTTPS floods, slow-rate attacks, and exploitation based on different categories. CIC-IDS2017 is important for analyzing the effectiveness of intrusion detection systems under the intensity of complex and dynamic network threats.

UNSW-15: This dataset is a relatively newer dataset in intrusion detection research, focusing on recent cyberattacks, especially backdoors. It offers a more realistic traffic mix compared to older datasets, helpful for testing intrusion detection systems against contemporary threats.

CICIOT 2023: It is a dedicated dataset for IoT security, encompassing a wide range of IoT-type attacks in the form of DOS/DDoS, reconnaissance, web-type attacks, brute force, spoofing, and Mirai attacks. Developing and testing intrusion detection systems for IoT environments required CICIoT2023.

DOI: 10.17148/IJARCCE.2024.131019

Table. 1 Comparison of various datasets

Dataset	Features	Rows	Attacks
KDD Cup'99	41	4,898,431	DOS, U2R, R2L, Probe
NSL-KDD	41	125,973	DOS, U2R, R2L, Probe
ISCXIDS	78	2,830,779	DOS, U2R, R2L, Probe, Web, Botnet, Reconnaissance
CIC-IDS2017	80	2,830,743	HTTP Flood, HTTPS Flood, Slowloris, Slowhttptest, Heartbleed, Botnet, Infiltration, PortScan, DDoS, Web Attack, Brute Force
UNSW-NB15	49	2,540,044	Fuzzers, Exploits, DoS, Reconnaissance, Generic, Shellcode, Backdoors
CICIoT2023	47	49,686,579	DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, Mirai

Type of Attackers: This differentiates between types of Attackers

External Attacker: An unauthorized individual outside of the organization that seeks to penetrate the network for the purpose of accessing sensitive information, disrupting services, or causing damage. External attackers typically use methods such as phishing, malware, and exploitation of vulnerabilities in the network to gain entry. Since they do not have direct access to internal resources, they rely on breaching security defences from an external perspective.

Internal Attacker: it could be the employee, contractor, or a business partner with authorized access to internal resources for malicious purposes. The internal attacker can steal protected data, alter or delete the information, otherwise sabotage systems. They are often significant threats since they gain privileged information and breach any external defence.

II. LITERATURE SURVEY

This literature survey explores recent advancements in intrusion detection and prevention systems using Machine learning and Deep learning techniques.

Table. 2 Literature survey

Ref.No.	Dataset & Techniques	Advantages	Limitations	Accuracy
[1]	UNSW-NB15 Anomaly-based detection	Identifying potential threats to security incidents.	Generate false positives	94%
[2]	Labeled network traffic Anomaly-based detection	Real-time monitoring, effective threat detection	It can generate false positives, struggle with encrypted traffic analysis	93%
[3]	CICIDS ARP Spoofing, MAC Flooding	Real-time monitoring, detailed insights into network behaviour	High data volumes leading to potential performance issues	92%
[4]	KDDCup ‘99 SVM	Reduces dimensionality, enhancing computational efficiency	Lose some important information during dimensionality reduction	97%
[5]	KDDCup ‘99 ABID and KBID	Effective threat detection	Challenges with dataset diversity	94%
[6]	NSL-KDD K-means, SOM	Effectively identify anomalies in network traffic, adapt to new patterns	High-dimensional data, require extensive computational resources	96%

[7]	UNSW-NB MLP classifier	Automatically learn complex patterns from large datasets, resulting in high detection accuracy	Requires substantial computational resources	98%
[8]	ACM, IEEE CNN, RNN	Superior detection accuracy and the ability to learn complex patterns in large datasets	require significant computational resources, extensive labeled training data	91%
[9]	KDD Cup SVM, Naive Bayes	Automatically adapt to new threats, improve detection accuracy, and reduce false positives	Require substantial labeled training data, face challenges with high-dimensional feature spaces	97%
[10]	NSL KDD, KAGGLE Naïve bayes, Random Forest	Enhance detection accuracy, reduce false positives	computationally expensive, require large labeled datasets	98%
[11]	KDDCUP 99 SVM, FSVM	Enhanced adaptability to evolving threats, improved classification accuracy, and reduced training time	high-dimensional data, requires careful tuning of fuzzy parameters	91%
[12]	KDD RF, Naive Bayes	Identification of the most effective models, enhances detection accuracy	Require large amounts of labeled training data, and might face challenges with algorithm interpretability	96%
[13]	KDD SVM, KNN	Enhances security by protecting sensitive patient information	Face challenges with data privacy, integration of diverse data types, and the complexity of accurately detecting threats in a constantly evolving healthcare environment.	96%
[14]	KDD Cup 1999 Neural networks	Enhancing network security by providing real-time monitoring.	Generate False Positives, require constant updates and maintenance	94%
[15]	NSL-KDD RF, DT	High detection accuracy, adapt to new and evolving threats, and reduce false positives.	Large amounts of labeled training data.	95%
[16]	ASNM TUN CNN, Random Forest, and Support Vector Machine	Improved detection capabilities across various attack types, enhancing the system's overall effectiveness and accuracy	class imbalance, increased complexity in model training and evaluation, higher risk of misclassifying similar attacks	95%
[17]	KDDCup'99, Kyoto2006+ Decision Tree, KNN, ANN, SVM, K-Mean Clustering	Improved Detection Accuracy, Reduced FP	Require extensive computational resources	95%

[18]	KDDCup'99 SVM, KNN	Innovations in detection accuracy, and the integration of advanced techniques	Challenges with scalability, handling encrypted traffic, evolving attack patterns,	93%
[19]	ISCX Gradient boosting, AdaBoost decision tree, GAN	Improved anomaly detection, leveraging generative models to identify novel threats with high precision	Require extensive training data	97%
[20]	NSL-KDD RF, MLP	Adaptability to changing attack patterns, and the ability to detect unknown and complex attacks.	High computational cost & High false positive rates	97%
[21]	KDD Cup 1999 Neural networks	Improved Detection Accuracy, Reduced FP, Resource Usage	Can struggle with scalability and real-time performance in dynamic vehicle environments.	97%
[22]	NSLKDD and CICIDS-2017 DT, SVM, RF	Improved Detection Accuracy, Reduced FP.	Increase computational complexity	96%

III. SYSTEM ARCHITECTURE

The proposed IDPS architecture is based on CICIOT 2023, which is a state-of-the-art dataset that involves network traffic data specifically crafted for cybersecurity analysis in an IoT environment. The process begins with a Data Preprocessing stage, which proves crucial for cleaning and getting the raw data ready. This step includes processes like data normalization, handling missing values, feature extraction, and transformation so that the dataset is structured and is ready for analysis. Good preprocessing decreases the noise content in the input and improves the quality so that sound foundations are set up for the application of ML and DL models next.

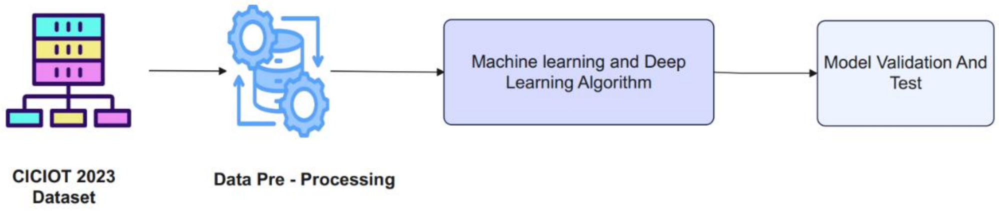
CICIOT 2023 Dataset
Data Pre - Processing
Machine learning and Deep Learning Algorithm
Model Validation And Test

Fig. 2 System architecture of IDPS

Once the data is pre-processed, it is fed to a set of algorithms used in Machine Learning and Deep Learning for intrusion detection purposes. These algorithms include, but are not limited to, supervised, unsupervised, and deep learning methods that are intended to learn malicious patterns and anomalies present in network traffic. After training, the best models are subjected to validation and testing to measure performances in terms of accuracy and precision, recall, as well as F1 measure. These metrics measure all the detection capabilities and stability of each model. Based on this validation, confidence is built that the system is sensitive enough to differentiate between normal operations and malicious activities, raising the reliability of the given IDPS in real environments of cybersecurity.

DOI: 10.17148/IJARCCE.2024.131019

IV. OBSERVATION AND FINDINGS

The survey highlights significant advancements in Network Intrusion Detection and Prevention Systems (NIDPS). The focus has shifted from traditional signature-based methods to more advanced machine learning (ML) and deep learning (DL) approaches. Models like Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and hybrid techniques are now widely used. These models have shown great effectiveness in accurately detecting various types of intrusions. however, such improvements bring along with them challenges of being quite compute-intensive and requiring large labeled datasets, especially for real-time systems.

Feature selection involves new approaches like Denoising Autoencoders and Multilayer Perceptron's which increase the accuracy but use less resources. Ensemble methods are ensemble learning methods, which combine Random Forest with other classifiers, further improving the detection but increasing complexity in the system. This method still poses issues in reducing false positives and dependency on labeled data.

The Intrusion Detection and Prevention System (IDPS) datasets are ranging from older ones like KDD Cup'99 to newer ones like CICIoT2023. These datasets vary significantly in terms of feature count (41–47), attack types (DoS, U2R, R2L, Probe, Web-based, Brute Force, Mirai, etc.) and dataset size (4.8 million to 49.9 million rows). This difference highlights the advancing scene of arrange assaults and the require for versatile IDPS. The huge dataset sizes offer potential for preparing vigorous machine learning models and dataset choice criteria are fundamental to draw authoritative conclusions.

Hybrid approaches combining anomaly and signature-based detection promise to reduce false positives and enhance threat identification. The overall survey points toward increased reliance on ML/DL techniques and feature selection and dimensionality reduction, while the challenges persist in computational cost, false positives, and ever-evolving threats. Continued innovation is in demand for scalable, real-time NIDS solutions.

V. CORE TAKEWAYS AND CHALLENGES

The key findings from the review of literature points out that machine learning (ML) and deep learning (DL) techniques have brought vast improvements to the detection accuracy, and models such as Random Forest, Support Vector Machines (SVM), and Convolutional Neural Networks (CNN) show results of between 91% and 98%. These progresses enhance real-time monitoring and adaptability in order to discern known and new threats. Ensemble learning methods further improved the detection performance by combining the strength of different models. Methods such as feature selection using Denoising Autoencoders (DAE) also optimized efficiency by diminishing data dimensionality. However, one of the most significant issues remains. For example, many deep learning models are very computationally intensive and therefore mostly fall within the space of real-time or resource-constrained application areas. Scalability is therefore a pressing need as the networks themselves generate more NIDS traffic without impacting the performance of these systems. False positives have many significant burdens, and one needs to build huge datasets for large models to train, which poses a great challenge in many of the specialized contexts. With these challenges, the effectiveness of NIDS should also continue to ward off zero-day attacks with evolving cyber threats. Network Intrusion Detection Systems, as these systems need to adapt constantly to new patterns of attack within a constantly shifting environment.

VI. CONCLUSION

This study examines how Machine Learning (ML) and Deep Learning (DL) are transforming Intrusion Detection and Prevention Systems (IDPS). Applying advanced techniques such as Random Forest, Support Vector Machine, and Convolutional Neural Networks, these systems have achieved detection accuracies between 91% and 98% across various datasets and attack types. The integration of these methods improves adaptability, reduces false positive rates and significantly improves threat detection. However, the challenges include high computational demands, dependency on large labeled datasets, and scalability issues.

This evaluation highlights the critical advancements that machine learning (ML) and deep learning (DL) bring to cybersecurity. By focusing on lightweight, efficient models capable of processing large-scale data and adopting hybrid approaches that combine anomaly-based and signature-based detection and prevention, IDPS can evolve into adaptive, strong defenses against both known and emerging threats, opening the door for future improvements in cybersecurity.

DOI: 10.17148/IJARCCE.2024.131019

VII. FUTURE SCOPE

In the future, Intrusion Detection and Prevention Systems (IDPS) can be enhanced with advanced deep learning models that combine high accuracy with low computational requirements, making them perfect for real-time use. Lightweight algorithms will be essential to handle growing network sizes and large data volumes without sacrificing performance. Cloud-based systems will improve scalability, allowing IDPS to work seamlessly across distributed networks. Efforts will focus on reducing false positives by using hybrid models that combine supervised and unsupervised learning for better precision. Deep learning techniques will also help streamline operations by selecting the most relevant features, reducing the need for extensive labeled data. To keep up with constantly evolving cyber threats, future IDPS will need adaptive, self-learning AI capabilities to detect and respond to zero-day attacks, paving the way for stronger, more reliable cybersecurity systems.

REFERENCES

[1]. Sherif, J. S., & Dearmond, T. G., "Intrusion Detection: Systems and Models," IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02), pp. 1080-1383, 2002.

[2]. Raghunath, B. R., & Mahadeo, S. N., "Network Intrusion Detection System (NIDS)," First International Conference on Emerging Trends in Engineering and Technology (ICETET), DOI: 10.1109/ICETET.2008.252, IEEE, ISBN 978-0-7695-3267-7, 2008.

[3]. Qadeer, M. A., Iqbal, A., Zahid, M., & Siddiqui, M. R., "Network Traffic Analysis and Intrusion Detection using Packet Sniffer," 2010 Second International Conference on Communication Software and Networks (ICCSN), pp. 313-317, DOI: 10.1109/ICCSN.2010.104, 2010.

[4]. Praneeth, N. S. K. H., Naveen Varma, M., & Roshan Ramakrishna Naik, "Principal Component Analysis Based Intrusion Detection System Using Support Vector Machine," IEEE International Conference on Recent Trends in Electronics Information Communication Technology (RTEICT), 2016.

[5]. Jubeen Shah, "Understanding and Study of Intrusion Detection Systems for Various Networks and Domains," 2017 International Conference on Computer Communication and Informatics (ICCCI-2017), IEEE, 2017.

[6]. Muder Almi’ani, Alia Abu Ghazleh, Amer Al-Rahayfeh, & Abdul Razaque, "Intelligent Intrusion Detection System Using Clustered Self Organized Map," International Conference on Software Defined Systems, IEEE, DOI: 10.1109/SDS.2018.8370392, 2018.

[7]. Hongpo Zhang, Chase Q. Wu, Shan Gao, Zongmin Wang, Yuxiao Xu, & Yongpeng Liu, "An Effective Deep Learning Based Scheme for Network Intrusion Detection," International Conference on Pattern Recognition (ICPR), pp. 978-1-5386-3788-3, 2018.

[8]. Sinem Osken, Ecem Nur Yildirim, Gozde Karatas, & Levent Cuhaci, "Intrusion Detection Systems with Deep Learning: A Systematic Mapping Study," Proceedings of the 2019 International Conference on Machine Learning and Applications (ICMLA), DOI: 10.1109/ICMLA.2019.0013, 2019.

[9]. Anish Halima A. & Sundara Kantham, K., "Machine Learning Based Intrusion Detection System," International Conference on Trends in Electronics and Informatics (ICOEI), IEEE Xplore, 2019.

[10]. Sivanantham, S., Abirami, R., & Gowsalya, R., "Comparing the Performance of Adaptive Boosted Classifiers in Anomaly-based Intrusion Detection System for Networks," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECON), DOI: 10.1109/ViTECON.2019.8899390, 2019.

[11]. Dong Yuan Tong, "Research of Intrusion Detection Method Based on IL-FSVM," 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2019.

[12]. Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M., "Evaluation of Machine Learning Algorithms for Intrusion Detection System," International Journal of Computer (IJC), vol. 38, no. 1, pp. 93-101, 2020.

[13]. Anar A. Hady, Ali Ghubaish, Tara Salman, Devrim Unal, & Raj Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," IEEE Access, vol. 8, pp. 116848-116861, 2020.

[14]. Raj Kishore & Anamika Chauhan, "Intrusion Detection System: A Need," 2020 IEEE International Conference for Innovation in Technology (INOCON), DOI: 10.1109/INOCON50539.2020.9298299, Nov 2020.

[15]. Usman Shuaibu Musa, Megha Chhabra, Aniso Ali, & Mandeep Kaur, "Intrusion Detection System Using Machine Learning Techniques: A Review," Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020), IEEE Xplore, pp. 149, DOI: 10.1109/ICOSEC49089.2020.9215372, 2020.

DOI: 10.17148/IJARCCE.2024.131019

[16]. Ajay Shah, Sophine Clachar, Manfred Minimair, & Davis Cook, "Building Multiclass Classification Baselines for Anomaly-based Network Intrusion Detection Systems," 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA), DOI: 10.1109/DSAA49011.2020.00102, 2020.

[17]. Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, & Farhan Ahmad, "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, 2021.

[18]. Kumar, S., Gupta, S., & Arora, S., "Research Trends in Network-Based Intrusion Detection Systems: A Review," IEEE Access, vol. 9, pp. 160324-160342, DOI: 10.1109/ACCESS.2021.3129775, 2021.

[19]. Taehoon Kim & Wooguil Pak, "Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier," IEEE Access, vol. 10, pp. 12450-12459, 2022.

[20]. Manvith Pallepati, Soujenya Voggu, Rithesh Masula, & Manisai Konjarla, "Network Intrusion Detection System Using Machine Learning with Data Preprocessing and Feature Extraction," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 10, issue VI, June 2022.

[21]. Jiangjiang Zhang, Bei Gong, Muhammad Waqas, Shanshan Tu, & Sheng Chen, "Many-Objective Optimization Based Intrusion Detection for In-Vehicle Network Security," IEEE Transactions on Intelligent Transportation Systems, DOI: 10.1109/TITS.2023.3296002, 2023.

[22]. Osvaldo Arreche, Ismail Bibers, & Mustafa Abdallah, "A Two-Level Ensemble Learning Framework for Enhancing Network Intrusion Detection Systems," IEEE Access, vol. 12, DOI: 10.1109/ACCESS.2024.3407029, 2024.