Fuse Guard: A Network Intrusion Detection System Using Machine Learning: A Review

Arsalan Ahmed Alyas
School of Computer Science & Engineering
Lovely Professional University
Phagwara, India
arslanahmed113@gmail.com

Kalikireddy Thapaswin Reddy
School of Computer Science & Engineering
Lovely Professional University
Phagwara, India
thapaswin125@gmail.com

Durga Sandeep Pavan Saladi
School of Computer Science & Engineering
Lovely Professional University
Phagwara, India
sandeeppavan2125@gmail.com

***Abstract*—Advanced intrusion detection systems (IDS) are required to protect digital assets against the ever-changing cyber threat landscape. Machine learning (ML), which learns from data and detects new threats, is at the forefront of this evolution. This paper studies the effectiveness of three main ML algorithms ML-K Nearest Neighbors (KNN), Bernoulli Naive Bayes (BNB), and Decision Tree Classifier (DTC) in IDS surveys from 2020 to 2024. In-depth analysis of different ML functions search, accuracy, and key performance metrics such as search speed, we provide comparative information about these algorithms. Our analysis highlights the strengths and limitations of each algorithm and highlights their most effective deployment scenarios in IDS. Furthermore, we identify important gaps in ML-based IDS research, such as increased scalability and adaptability, and suggest future research directions. This study provides a reference for practitioners as well as researchers in adopting and upgrading ML algorithms to develop effective IDSs, incorporating to the larger conversation about the use of these technologies. IDS using machine learning.**

***Keywords*—*Intrusion Detection System, Machine Learning, K-Nearest Neighbors, KNN, Bernoulli Naive Bayes, BNB, Decision Tree Classifier, DTC, Cyber Security, Algorithm Comparison, Research Gaps*.**

I. Introduction

In the era of digital transformation, cybersecurity has emerged as a serious problem for enterprises globally as the complexity and frequency of cyber threats increase, the need for advanced defence mechanisms becomes undeniable. Intrusion detection systems (IDS) are an important part of this line of defence and are intended to prevent unauthorized access and malicious activities to the network and system environment. However, the dynamic and evolving nature of cyber threats often exceeds the capabilities of traditional IDSs, which are supported by fixed rules and hampered by an inability to adapt to new and unseen attacks.

Enter the realm of machine learning (ML), a revolutionary force that is redefining intrusion detection. Using ML algorithms, IDS can overcome traditional limitations to identify complex patterns and predict future intrusions with high accuracy. The growing interest in ML in cybersecurity highlights the collective efforts to strengthen IDS against a wide range of cyber threats.

This paper describes three important ML algorithms: K-Nearest Neighbors (KNN), Bernoulli Naive Bayes (BNB), and Decision Tree Classifier (DTC). Each of these presents distinct strengths and challenges for intrusion detection. From the simplicity and effectiveness of KNN classification to BNB's skill with binary data to transparent DTC decision-making, these algorithms provide a variety of strategies to improve IDS performance.

The purpose of this paper is to outline the role and impact of these algorithms in IDS, provide a detailed comparative analysis, and assess the benefits, limitations, and contextual dynamics that shape their deployment. Through this study, we seek to explore the optimization paths of these ML algorithms in intrusion detection and provide insights that may guide the future direction of IDS evolution.

A. Intrusion Detection Systems (IDS):

An intrusion in the digital realm is an unauthorized entry or harmful activity in a computer system. Intruders aim to access confidential data or perform malicious actions. To combat this, Intrusion Detection Systems (IDS) are deployed. Their primary role is to detect and alert on unauthorized or suspicious activities happening within a system, serving as a critical component of computer security.

B. Role of Intrusion Detection System:

IDS serve as vigilant guardians of computer systems, actively searching for a range of malicious activities that could signify an attack. They are essential tools in the cybersecurity arsenal, helping to maintain the integrity and security of our digital environments. By identifying potential threats, IDS play a crucial role in protecting systems from unauthorized access and potential damage.

TABLE I. Common Attacks on TCP/IP Models With Their Relevance.

TCP/IP Layer	Common Attacks	Relevance
Application Layer	Phishing, Web based attacks, injection.	ML can analyze content patterns to detect malicious intent.
Transport Layer	SYN Flood, Port Scanning.	ML can identify anomalous packet sequences and flag DDoS.
Network Layer	IP Spoofing, Ping of Death.	ML can monitor IP anomalies and unusual ping packets.
Data Link Layer	ARP Spoofing, MAC Flooding.	ML can detect irregularities in MAC addresses and ARP traffic.
Physical Layer	Eavesdropping, Tampering	ML is less used at this layer but can assist in anomaly detection based on signal patterns.

II. ARCHITECTURE OF IDS

An effective IDS is structured around a core architecture that ensures comprehensive monitoring, detection, and response to potential threats [6]. The architecture can be delineated into four integral components, each playing a pivotal role in the IDS's functionality:

A. Data Collection:

This foundational component involves the aggregation of data from various sources within the network or system. The data collected can include network traffic, system logs, application logs, and other relevant data streams that may contain indicators of potential security incidents.

B. Feature Selection:

Following data collection, the IDS processes the data to extract and select pertinent features or attributes that are crucial for identifying suspicious activities[8]. This step involves filtering out irrelevant data and focusing on the information that is most indicative of potential threats, thereby optimizing the analysis process for speed and accuracy.

C. Analysis:

The core analytical engine of the IDS examines the selected features using sophisticated algorithms to identify patterns or anomalies indicative of intrusions or malicious activities. This is where machine learning algorithms—such as KNN, BNB, and DTC—play a critical role, leveraging their ability to learn from data and improve threat detection over time[4].

D. Action:

Based on the results of the analysis, the IDS takes predetermined actions to mitigate the threat. These actions can range from generating alerts to inform system administrators of potential intrusions to triggering automatic response mechanisms designed to block or contain the threat. By following these steps, an IDS can effectively detect unusual or unauthorized activities, providing a crucial layer of security for computer systems and networks.

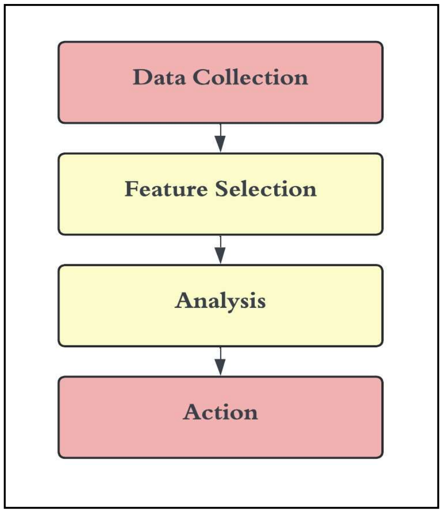

Fig1. Architecture of IDS

The Fig1. illustrates the IDS architecture, encompassing these four components, providing a visual representation of how an IDS functions to detect and respond to cybersecurity threats.

III. APPLICATIONS AND CHALLENGES

A. Applications

- Cloud Computing and IoT Security: The Proliferation of cloud computing and IoT has introduced a novel protection challenges, necessitating sturdy NIDS. The study [2] demonstrates on how device mastering-greater NIDS can substantially improve protection protocols in cloud environments, addressing unique threats inherent to those systems.
- Smart Grid Protection: With the increasing digitalization of application infrastructures, smart grids have become high targets for cyber-assaults. The application of system gaining knowledge of in NIDS, as explored inside the study [3], performs a pivotal position in detecting and mitigating threats in those important systems, showcasing the adaptability of NIDS to sector-precise necessities.

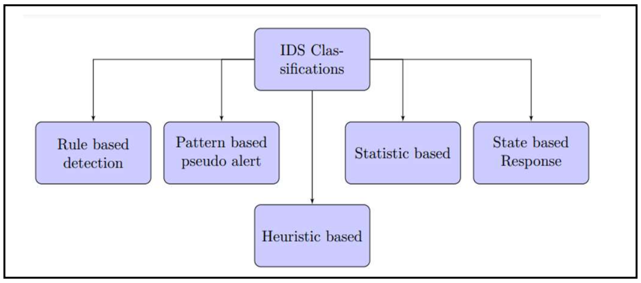

Fig2. Classification of IDS

B. Challenges

- Algorithm Optimization: The effectiveness of NIDS is noticeably dependent on the choice of system learning algorithms. Selecting and optimizing the proper algorithm is hard yet crucial for balancing accuracy and computational performance [1]. This stability is critical for actual-time risk detection and reaction in network protection.
- Data Quality and Imbalance: High-first class and nicely balanced data are critical for schooling effective machine gaining knowledge of models for NIDS. Studies [2] highlight the demanding situations in records instruction, inclusive of addressing information imbalance and making sure that the education statistics appropriately represent the community traffic and risk eventualities.
- Adaptation to Evolving Threats: Cyber threats usually evolve, with attackers continuously growing new methods to bypass security features. Machine getting to know models utilized in NIDS need to adapt to these changes to stay effective [1]. This adaptability is

essential for retaining the relevance and effectiveness of NIDS inside the face of latest and sophisticated cyber threats.

- Real-Time Processing Requirements: NIDS ought to examine and reply to threats in actual-time or near-actual-time [6]. Integrating system studying models that could method and examine statistics unexpectedly at the same time as retaining high detection accuracy poses an extensive project [12]. The real-time requirement is important for NIDS to effectively mitigate threats and save you capacity breaches.

IV. Literature Review

R.Dutta et al. [1] has provided a meticulous examination of machine learning algorithms applied to Intrusion Detection Systems (IDS), delving into a comparative analysis to discern the most effective techniques for real-world applications. Dutta et al. meticulously dissected the performance of various ML algorithms across several metrics, offering a granular view that aids in identifying the optimal strategies for different network environments. Their research stands out for its thoroughness in evaluating algorithmic performance, providing a foundational resource for cybersecurity professionals seeking to leverage ML for enhanced network protection. Research Gap: Future studies could delve into the contextual efficacy of these ML algorithms, assessing their performance across a spectrum of network scenarios to provide a more nuanced understanding of their applicability.

V. S. A. Raju et al. [2] In response to the escalating threat landscape in IoT networks, their research focuses on deploying ML algorithms to detect IoT-botnet attacks, a burgeoning concern in cybersecurity. The study not only underscores the adaptability of ML in identifying complex threat patterns but also emphasizes the tailored application of these algorithms for IoT-specific challenges. Their work contributes a crucial piece to the puzzle in securing IoT ecosystems, demonstrating the effectiveness of ML in thwarting sophisticated botnet intrusions. Research Gap: A potential research direction is the examination of ML algorithms' effectiveness across the diverse spectrum of IoT devices and the development of more granular, device-specific IDS models.

Magán-Carrión et al. [3] focuses on the integration of multiple datasets to bolster the reliability of IDS is at the core of research. By amalgamating diverse data sources, they address the critical issue of data scarcity and imbalance, enhancing the ML models' ability to generalize and accurately detect intrusions across varied network scenarios. This innovative approach not only enhances the detection capabilities of IDS but also sets a new benchmark for dataset utilization in ML-driven cybersecurity solutions, offering a novel methodology that could shape future research directions. Research Gap: Future work could explore methodologies to ensure data consistency and address potential biases in integrated datasets, enhancing the robustness of dataset integration strategies.

A. Hussain et al. [4] exploration into a NIDS capable of identifying both known and emerging zero-day anomalies highlights the proactive potential of ML in cybersecurity. By developing systems that can adapt to and recognize new threat patterns, their research underscores the imperative for IDS to evolve in tandem with the cyber threat landscape. This study is particularly significant for its focus on zero-day anomaly detection, offering insights into the development of advanced, future-proof intrusion detection systems. Research Gap: Investigating the long-term adaptability of ML models in NIDS and developing frameworks for continuous learning and model evolution in response to new threats would be a valuable area for further research.

R. Kumar et al. [5] delve into the specifics of implementing ML algorithms within a NIDS framework, offering an in-depth look at the system's architecture, algorithm selection, and performance evaluation. Their comprehensive analysis provides a blueprint for effectively deploying ML-based IDS, highlighting crucial considerations and best practices that can inform the design and operation of such systems, thereby enhancing their efficacy and efficiency in real-world settings. Research Gap: Further research could explore the user experience and system integration aspects of ML-based NIDS, enhancing their usability and effectiveness in real-world network settings.

G. Kaur et al. [6] focused on the automation of machine learning-enabled IDS. By automating the ML process, their novel technique aims to enhance the speed and responsiveness of IDS, minimizing the need for manual intervention and enabling quicker responses to potential threats. This study is notable for advancing the conversation on automation in ML for IDS, pointing toward a future where IDS can operate more autonomously and effectively. Research Gap: Future research could focus on the challenges of automation in ML for IDS, particularly exploring mechanisms to maintain system transparency and interpretability while automating the detection process.

N. Varghese et al. [7] Investigates the effectiveness of ensemble ML models in IDS, Varghese and Vivek provide a compelling case for the superiority of these models over single-method approaches. Their research, utilizing the KDDCup 99 dataset, showcases how ensemble methods can enhance detection accuracy and system reliability, offering a persuasive argument for the integration of ensemble learning in the development of robust NIDS. Research Gap: An area for future exploration could be optimizing ensemble models to reduce computational demands while maintaining or enhancing detection accuracy.

T. Kim et al. [8] Focused on the critical need for speed in intrusion detection, they developed an ML-based NIDS that emphasizes early classification. Their system demonstrates how early detection and classification can significantly reduce the time to respond to intrusions, highlighting the importance of timeliness in mitigating the impact of network breaches and enhancing the overall security posture of networked systems. Research Gap: Further studies could investigate the trade-offs associated with early classification in ML-based networked systems. Research Gap: Further studies could investigate the trade-offs associated with early classification in classification in ML-based NIDS, aiming to optimize the balance between speed and accuracy.

Mhamdi et al. [9] Targeted the unique domain of software-defined networks. applied deep and machine learning techniques to create a sophisticated intrusion detection framework. Their work illuminates the potential for leveraging the inherent flexibility of SDNs to implement advanced ML models, providing a forward-looking perspective on how intrusion detection can evolve in conjunction with emerging network technologies. Research Gap: Future research might focus on the seamless integration of ML-based IDS within SDNs, ensuring that the deployment does not introduce new vulnerabilities or compromise network performance. This also doesn't enhance the detection rate while there are other systems which produce with high accuracy rates within less time and enhanced detection techniques.

Vinoth Y. et al. [10] presents a sophisticated anomaly-based network intrusion detection framework that leverages the strength of ensemble machine learning techniques. By integrating diverse algorithms, this approach aims to enhance the robustness and accuracy of intrusion detection, effectively reducing false positives and improving the system's reliability in dynamic network environments. The study not only demonstrates the ensemble method's superior performance over single-model approaches but also emphasizes the importance of diversified analytical strategies in tackling complex intrusion patterns, offering a comprehensive blueprint for future advancements in anomaly detection. Research Gap: while the whole point of exploration is on ensemble machine learning techniques in NIDS, the study doesn't deeply assess the models' performance in real-world network conditions.

The TABLE II illustrates a comparison of various studies focusing on the different algorithms through Machine Learning and Deep Learning. The study is evaluated based on the datasets used, algorithm used, accuracy of the model, the advantages and limitations noted. In short, this table is a summary of the recent advancements in the IDS, the strategies used to tackle various attacks.

TABLE II. COMPARATIVE ANALYSIS OF VARIOUS STUDIES ON IDS.

Ref	Objective	Dataset Used	Algorithm Used	Accuracy	Advantages	Limitations
[1]	Creating an effective and reliable intrusion detection model.	NSL -KDD	NBC, DTC, K-NN, Logistic Regression	0.9977%	Provides a reduced false alarm rate while keeping a high diagnosis rate.	Overfitting, which is essential for the model to generalize to new data, is not sufficiently addressed in the work.
[2]	To enhance IoT security by applying machine learning to detect and mitigate IoT-Botnet attacks	CIC IoT Dataset 2023	DTC, RFC, K-NN	99.17%	Offers the potential for improved detection of novel and variant attacks that traditional methods might miss.	The potential for false positives or negatives, and the requirement for continuous training with new data to maintain effectiveness.
[3]	To provide R-NIDS, a machine learning (ML) NIDS that enhances the generalization of intrusion detection.	UGR'16, USNW-NB15 and NLS-KDD	Multinomial Logistic Regression (LR) and Random Forest (RF)	0.9067%	Adding more datasets to a model enhances its generalization and robustness in network intrusion detection.	Despite dataset integration, performance inconsistency between multiple datasets is still a problem.
[4]	Enhance NIDS by combining OC-SVM and RF for detecting various attacks.	CSE-CIC-IDS-2018	OC-SVM, RF	95.95%	Efficiently detects known and zero-day attacks.	Potential challenges with new attack vectors and false positives.
[5]	Improve IoT NIDS using various ML methods.	KDD	KNN, SVM, LR, RF, DT, NB	high	Detects known/unknown attacks efficiently.	Lacks IPS; identifies but doesn't prevent.
[7]	Evaluate ensemble ML models for network intrusion detection on KDDCup 99 dataset.	KDDCup 99	NB, LR, DT, RF, GB, SVM, ANN.	99.969%	Demonstrates the effectiveness of ensemble models, especially RF, in intrusion detection.	Limited to the KDDCup 99 dataset; bigger datasets may provide scalability concerns.
[8]	Enhance ML-based NIDS via early session classification.	ISCX2012, CIC-IDS2017, CSE-CIC-IDS2018	RF, AdaBoost DT, XGBoost, ELM, DNN, CNN	94.21%	Increased detection accuracy and speed.	Inconsistent improvements across classes/algos.
[9]	Enhance NIDS in SDN using ML and DL models.	NSL-KDD	KNN, Naive Bayes, SoftMax, SVM, DNN	87.72%	High accuracy in multiclass classification.	Lower accuracy in certain attack categories.
[11]	To implement ML algorithms for enhancing network intrusion detection.	-	Decision Tree, Logistic Regression, Random Forest, SVM	-	Improved detection rates, effective for various attack types.	Not all algorithms performed equally well while some had lower accuracy.
[12]	Enhance NIDS for DHCP Attacks	Custom	Random Forest, KNeighbors, Extra Tree, Linear SVC	99.32%	Targeted DHCP, DoS detection, Realistic dataset Effective classification	Limited to DHCP, Scalability in broader networks possible
[13]	Develop a hybrid ML and DL model to improve network intrusion detection rates.	KDDCUP' 99, CIC-MalMem-2022	SMOTE + XGBoost	99.99%-KDD, 100% – CIC-MalMem	Improved detection rates, dependable and effective for real-time implementation in IDS devices	The limitation is the study's specificity to the datasets used

[14]	Enhance IDS for imbalanced data	NSL-KDD	CTGAN, SVM, KNN, DT	-	Improved F1-score, G-mean for SVM, DT.	Limited KNN improvement due to class imbalance insensitivity.
[15]	Enhance IDS performance	NSL-KDD, UNSW-NB15	Decision tree, Local Outlier Factor	R2L: 99.89%, U2R: 99.22%, UNSW-NB15: 91.86%	High accuracy, efficient feature selection and data reduction	Needs improved sensitivity, specificity, handling imbalanced data
[16]	Develop an adaptive and resilient IDS using deep learning	UNSW-NB15	Deep Learning (CNN with multi-layer perceptron)	-	Capable of detecting recognized and zero-day network threats	-
[17]	Enhance cloud intrusion detection with collaborative ML.	UNSW-NB15	Ensemble Boosted Trees, Complex Trees	80.43%	Combines two ML algorithms. Detects and identifies attack types.	handling new attack types, large data volume management, and class imbalance.
[18]	Detect and classify network attacks	CSE-CIC-IDS2018	MLP, RF, KNN, SVM, AdaBoost, Naive Bayes	99.97%	High accuracy	challenges with zero-day attacks, overfitting, and the need for ongoing model updates.
[19]	Enhance cloud intrusion detection using deep and shallow learning.	KDD Cup 99, NSL-KDD.	SCAE, SVM.	98.11%	Improved detection, effective feature extraction.	May struggle with unknown attacks, risk of overfitting.
[20]	Enhance IoT security through anomaly detection	IoT Network Intrusion Dataset	KNN	99%	Efficient detection of anomalies.	Limited comparison of algorithms.
[21]	Compare data mining methods for IDS and suggest improvements.	NSL-KDD, UNSV-NB15	ACO, SVM, Genetic algorithms, CNNs, Deep networks, Ensemble methods	ACO: 99.5%, SVM: 95.8%, Genetic: 99.9%, Hybrid: 99.2%.	High accuracy.	Challenges in optimal feature selection and subset attainment.
[22]	Develop an IDS using deep learning for better IoT security.	-	Fuzzy CNN	improved	Higher detection accuracy, efficient DoS detection, lower false positives.	High latency, increased resource consumption.

V. Discussion

The study review discusses how machine learning (ML) algorithms hold potential in enhancing intrusion detection systems (IDS) to combat cyber threats effectively. It underscores the significance of using a mix of ML and deep learning methods to enhance the adaptability and precision of IDS in detecting threats. The integration of Network Intrusion Detection System (NIDS), with Host Intrusion Detection System (HIDS) is seen as an approach to enhancing anomaly detection capabilities. Standardized methodologies play a role in evaluating and comparing ML driven IDS technologies while real world validation ensures their dependability. Moving forward continuous research is essential to address the evolving cybersecurity challenges emphasizing the development of ML based IDS for safeguarding digital assets.

VI. Conclusion and Future Scope

Machine learning (ML) algorithms integrated into intrusion detection systems (IDS) represent significant progress in cyber security, threat detection in the system allows the evaluation of IDS through ML techniques and applications, this review paper shows the transformative impact of ML-based system in strengthening cyber security defence While providing the advantages, limitations, and future prospects of IDS, this study provides various valuable insights for the researchers and practitioners seeking to explore the complexity of cyber threats to address challenges such as adversaries, attacks, developing model-defined capabilities;
Exploring hybrid ML deep learning methods and standardization methods is an important step to advance in this field. As the cybersecurity landscape evolves day by day, the integration of ML with various algorithms into IDS is going to play a key role in protecting digital assets and mitigating emerging threats.

The future objective of this study is to integrate Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS) as one Intrusion Detection System (IDS). This integration through both NIDS and HIDS promises to be able to provide anomaly detection and has improved with the combination. Key areas to explore include developing hybrid detection algorithms, maximizing and scalability of resources, incorporating machine learning for dynamic threat optimization Validation through extensive testing in simulated and real-world contexts Practical practices and performance in in different deployment scenarios is important for decision making.

References

[1] R. Dutta, B. K. Nirupama and Niranjanamurthy, "Intrusion Detection System (IDS) Analysis Using ML," 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru,India,2022,pp.14,doi:10.1109/MysuruCon55714.2022.9972442.

[2] V. S. A. Raju and S. B, "Network Intrusion Detection for IoT-Botnet Attacks Using ML Algorithms," 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2023, pp. 1-6, doi: 10.1109/CSITSS60515.2023.10334188.

[3] R. Magán-Carrión, D. Urda, I. Diaz-Cano and B. Dorronsoro, "Improving the Reliability of Network Intrusion Detection Systems Through Dataset Integration," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 1717-1732, 1 Oct.-Dec. 2022, doi: 10.1109/TETC.2022.3178283.

[4] A. Hussain, F. Aguiló-Gost, E. Simó-Mezquita, E. Marín-Tordera and X. Massip, "An NIDS for Known and Zero-Day Anomalies," 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 2023, pp. 1-7, doi: 10.1109/DRCN57075.2023.10108319.

[5] R. Kumar and A. H. Nalband, "Network Intrusion Detection System using ML," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 2490-2495, doi: 10.1109/ICAC3N56670.2022.10074106.

[6] G. Kaur, A. Gupta and H. K. Saini, "A Novel Technique for Automized ML-Enabled IDS," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 490-498, doi: 10.1109/CICTN57981.2023.10140603.

[7] N. Varghese and R. Vivek, "The Efficiency of Ensemble Machine Learning Models on Network Intrusion Detection using KDDCup 99 Dataset," 2023 IEEE International Conference on Contemporary Computing and Communications (InC4), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/InC457730.2023.10263037.

[8] T. Kim and W. Pak, "Robust Network Intrusion Detection System Based on Machine-Learning With Early Classification," in IEEE Access, vol. 10, pp. 10754-10767, 2022, doi: 10.1109/ACCESS.2022.3145002.

[9] L. Mhamdi, H. Hamdi and M. A. Mahmood, "Network Intrusion Detection in Software-Defined Network Using Deep and Machine Learning," GLOBECOM 2023 - 2023 IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 2023, pp.2692-2697,doi:10.1109/GLOBECOM54140.2023.10437050.

[10] Vinoth Y. and Kamatchi K. (2020). Anomaly Based Network Intrusion Detection using Ensemble Machine Learning Technique. International Journal of Research in Engineering, Science and Management. IJRESM. (290-296).

[11] Ponthapalli . Raviteja, Mandapati. Satya Venkata Sarojini Devi, Mukka . Gowri, Majji. Vamsi Sai Krishna, P V S Prabhakar . (2020). Implementation of Machine Learning Algorithms for Detection of Network Intrusion. International Journal of Computer Science Trends and Technology (IJCST). (163 -169).

[12] S. Syed, F. Khuhawar and S. Talpur, "Machine Learning Approach For Classification of DHCP DoS Attacks in NIDS," 2021 IEEE 18th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Karachi, Pakistan, 2021, pp. 143-146, doi: 10.1109/HONET53078.2021.9615392.

[13] Talukder, Md. Alamin & Hasan, Fida & Islam, Manowarul & Uddin, Md Ashraf & Akhter, Arnisha & Yousuf, Mohammad & Alharbi, Fares & Moni, Mohammad Ali. (2022). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. 10.48550/arXiv.2212.04546.

[14] Alqarni AA, El-Alfy ESM. Improving Intrusion Detection for Imbalanced Network Traffic using Generative Deep Learning. International Journal of Advanced Computer Science and Applications. 2022;13(4):959-967. doi: 10.14569/IJACSA.2022.01304109

[15] Megantara, Achmad Akbar, and Tohari Ahmad. "A hybrid machine learning method for increasing the performance of network intrusion detection systems." Journal of Big Data 8.1 (2021): 1-19.

[16] Ashiku, Lirim, and Cihan Dagli. "Network intrusion detection system using deep learning." Procedia Computer Science 185 (2021): 239-247.

[17] Chkirbene, Zina & Ridha, Hamila & Erbad, Aiman & Kiranyaz, Serkan & Al-Emadi, Nasser & Hamdi, Mounir. (2021). Cooperative Machine Learning Techniques for Cloud Intrusion Detection. 837-842. 10.1109/IWCMC51323.2021.9498809.

[18] Kanimozhi, V., and T. Prem Jacob. "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing." ICT Express 7.3 (2021): 366-370.

[19] W. Wang, X. Du, D. Shan, R. Qin and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1634-1646, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3001017.

[20] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan and S. Khorsandroo, (2020, August). Anomaly Detection on IoT Network Intrusion Using Machine Learning. In 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-5). IEEE.

[21] Ahmad, Zeeshan, et al. "Network intrusion detection system: A systematic study of machine learning and deep learning approaches." Transactions on Emerging Telecommunications Technologies 32.1 (2021): e4150.

[22] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, “A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things,” Computational Intelligence and Neuroscience, vol. 2023, pp. 1–24, Jan. 2023.