Intrusion Detection Systems in Cybersecurity: A Critical Analysis Of ML-Based Approaches

Saurabh Kumar Singh[1], Kumar Amrendra[2], Sumit Kumar Pandey[3]
[1]*Research Scholar, Jharkhand Rai University*
[2]*Assistant Professor, Jharkhand Rai University*
[3]*Associate Professor, Jharkhand Rai University*
doi.org/10.64643/IJIRT208505

***Abstract*—Due to the advances of information and communication technology (ICT) together with its infrastructures or the modern digital society on which they rest, Simultaneously, there has been a multitude of advanced cyber-attacks occurring more frequently anywhere in the world against organizations, companies, governments, and civilians. This has made Intrusion Detection Systems (IDS) a critical part of safeguarding the cyberspace, since it allows to identify access without permission and hostile actions in an enterprise network. Signature-based IDS techniques are effective against known threats, but they are ineffective in identifying new or unknown or ever-evolving attack patterns which reduces the reliability of these techniques in dynamic environments. This limitation has led to a trend in creating Machine Learning (ML) techniques which listen to network traffic and learn high variety behavior patterns. In general, traditional machine learning algorithms have still been the most used class of tools nowadays for research in intrusion detection because they are easy to understand perform well with low computational cost and can be deployed into practice. The entire existing classical machine learning methods used in IDS (Decision Trees, Random Forests, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN) classifier, Naïve Bayes and Logistic Regression) are humorously described with great detail. The next step is then to review literature to characterize their performance, before detailing their strengths and weaknesses. In addition, the future directions also explore recent efforts on both current research lags as well as challenges / trends in intrusion detection. Although ensemble methods generally outperform, no algorithm on its own is able to solve all the challenges involved in complex cybersecurity. Hence, future research still needs attention towards the development of Adaptive, Explainable and Scalable IDS frameworks.**

***Index Terms*—Intrusion Detection System, Machine Learning, Cybersecurity, Random Forest, Support Vector Machine, Network Security, Anomaly Detection.**

I. INTRODUCTION

Digital technologies are creation, innovative communication and integration of knowledge-based activities. As organizations expand their footprint for critical operations on interdependent networks, cloud computing platforms, Internet of Things (IoT) devices and distributed information systems are likewise integrated into business practices. While these technologies have improved efficiency and accessibility in the workplace, they also come with serious security risks that malicious actors can exploit.[1]A lot has happened in how we measure cyber-attacks - both in terms of their number and complexity. Even if malware and unauthorized access attempts are still some of the biggest threats, in several instances even more sophisticated attack vectors with new types of threat actor techniques (e.g., ransomware or DDoS attacks, APTs or even phishing campaigns) have become fairly common [3].

One by one, cybersecurity has become a major concern for the entire world organizations and these attacks ends up in huge monetary losses, operational disruptions and even loss or theft of sensitive information also [4]. This resulted in the development of systems for detecting intrusion (Intrusion Detection Systems (IDSs)) and so Intrusion Detection Systems (IDSs) became an essential type of security system using which detection of suspicious behaviour occurred inside network zones. The traditional IDS solutions can generally be categorised in two major classes which are signature-based or anomaly-based. Signature-based systems are able to detect attacks of known types but do not help uncover zero-day exploits as well as even worse new attack patterns [5], [6]. To make up for these drawbacks, anomaly-based methods

are widely utilized because they understand the usual activities of the network and specify those non-connections which were malicious [7]. Non-MATLAB classiest the rise in network datasets along with improvements in computational technologies, machine joining methods that automatically take up incoming packets have kept pace. In contrast, machine learning algorithms are capable of monitoring large volumes of data, discovering new patterns that were not previously identified and adapting much more quickly to the evolution of threats than traditional rule-based detection systems [8]. History of Intrusion Detection Various algorithms such as Decision Trees, Random Forest, Support Vector Machines, k-Nearest Neighbor (kNN), Naïve Bayes and Logistic Regression have been examined for intrusion detection [9], [10].

Out of these methods, Random Forest and Support Vector Machines performed well on detection while Naïve Bayes and Logistic Regression are still relevant in resource-limited context because they can be computationally inexpensive [11]. Different real implementations can be assessed and contrasted through benchmark datasets [12], such as NSL-KDD, UNSW-NB15 [13] and CICIDS2017.

Even though many advances have been made, some issues remain unsolved such as class imbalance, concept drift, adversarial attacks and scalability [14]–[16]. Hence, it is very important to study traditional machine learning techniques in order to build an effective and reliable intrusion detection. This paper presents: (i) a survey of major machine learning algorithms used in IDS, including the strengths and weaknesses of these approaches; (ii) identifies research gaps that exist; and (iii) discusses the future paths that intelligent cybersecurity solutions might explore [17], [18].

II. REVIEW OF LITERATURE

Throughout the last decade till current years the application of machine learning methods in the field, or domain of intrusion detection systems [14] has been a research interest, for many researchers as previously mentioned the cyber-threat landscape is constantly changing and becoming not only more complex but also increasingly frequent to occur, so it's hard for traditional signature detection methods to detect new (previously unexplored) type of attack pattern/communication type. Accordingly, researchers have taken a variety of machine learning approaches so that the adaptability and intelligence of this type of intrusion detection framework can be further extended.

Ahmed et al. were among the earliest to thoroughly study anomaly-based intrusion detection. [1], Martin G. Sanchez, From Rule-based System to Machine Learning-driven Detection Systems for HCI Paradigms. The study emphasized the ability of machine learning algorithms to learn abnormal network activity without any attack signature defined with prior knowledge. The authors also stressed that adaptive learning methods have the potential to provide important performance increases in detection within rapidly changing network contexts.

In this regard, works discussed aimed for proposing new strategies in regards of the network traffic features and anomaly detection methods by Moustafa & Slay [2]. They showed that feature engineering is a key component in enhancing the accuracy of intrusion detection. The study also emphasised for choosing effective network attributes as extraneous features typically will increase computational cost without providing much benefit to classification accuracy.

Additionally, the creation of benchmark datasets further propelled research efforts in this area. Tavallaee et al. The NSL-KDD dataset [3] is a refined version of the standard KDD Cup 99 dataset. A prior work proposed reduced dimensionality PC-IRT [6] is even used to address our dataset limitations, including duplicate records and bias in distributions of data that provide a fairer described environment for testing intrusion detection algorithms. NSL-KDD remains one of the most-used datasets to evaluate machine learning based IDS algorithms ever since its introduction.

The decision trees-based methods have always been gaining interest due to their straightforward representation and ease of implementation. Chandrasekaran and Meena [4] analyzed different Intrusion Detection Techniques {and} stated that the Decision Trees yields good classification performance with low running time, while allowing to provide an understandable description of the underlying reasons for decisions. The authors argued that interpretable models are useful in cybersecurity environments because security analysts need to understand the

rationale behind alerts. Nancharaiah et al. also reported similar findings They were able to show how Decision Tree classifiers extract information from relatively rough data (typically used in classification problems) and give the opportunity to adapt them for other types of tasks.

Random Forest classifiers have become one of the most popular methods of intrusion detection using machine learning. The Random Forest algorithm was developed by Breiman [6] and is an ensemble learning method that brings together many decision trees to improve classification. Later research showed how Random Forest could be used in cyber security contexts [19]. Zhang et al. A three-branch Random Forest intrusion detection model was proposed and considerable improvements in attack classification performance were achieved through [7]. They concluded that ensemble learning reduces overfitting while improving generalization capabilities.

More et al. A big analysis of the UNSW-NB15 dataset [8] showed that Random Forest was always better than individual classifiers. Their research confirms that Random Forest is more resistant than the rest of algorithms against noise data and able to choose relevant features automatically which will improve the performance of attack detection. Similarly, Pinto et al. Random Forest: Random Forest is one of the most powerful classifiers for intrusion detection [9] as it provides a good trade-off between accuracy and computational complexity. Support Vector Machines (SVM)are also widely researched methodology for intrusion detection system. SVM is originally introduced by Cortes and Vapnik [10], which provides a strong classification framework in high-dimensional feature space. Building on this work, Aydin and Duman [11] established the SVM achieves a comparable level of detection accuracy across stomach-type intrusion detection datasets. The kernel functions in SVM take the separate, more complex non-linear relations or several network features and detect the cyberattacks effectively.

While SVMs are capable of learning perfect classifiers, in practice there are many limitations. In the large environment, an explosion of traffic is a heavier work for both the training and computing resources. Immastephy and Punitha [12] pointed out that SVM has a better performance over simpler types of classifiers, but the training time could prevent deploying in real-time. Therefore, recent works are extensively focused on optimizing methodologies to decrease the training and inference cost while achieving an acceptable model performance for detection. We have seen K-Nearest Neighbors (KNN) which is one of the simplest yet powerful algorithms, getting a lot of attention. Theoretical foundation for K-Nearest Neighbours (KNN) algorithm which uses similarity to neighbouring samples for instance classification was provided by Cover and Hart [13]. KNN has been successfully used as a classifier for malicious traffic in intrusion detection based on similarity-based measures [4] of network traffic. Sharma et al. KNN is very efficient in the detection of well-known types of attacks, but also very expensive on a bigger dataset [14] which summarizes its uselessness to apply on large-scale real-time intrusion detection systems. Naïve Bayes has been popular though – being computationally abled, effective and a probabilistic classifier. Domingos and Pazzani [15] showed that Naïve Bayes could do surprisingly well despite its assumption of feature independence. The algorithm is used in fast as an initial filtering due to its low computational overhead for anomaly detection applications in cybersecurity. Also, relatively insignificant detection performance with lesser computational needs has been reported in several studies, thereby claiming that it is a suitable method for resource-poor environment [14], [16].

Note: Logistic Regression is another prominent classification algorithm used in intrusion detection due to its straightforward nature, interpretability, and probabilistic prediction ability. It has shown good results for binary classification of normal and malicious traffic [17]. But it fails to model the higher complexity and non-linear attack pattern that comes with more sophisticated cyber threat.

The recent rise of deep learning-based technologies attracted a great deal of research attention in complex intrusion detection systems. Ng et al. Yum et al. [18] conducted an expansive survey of deep learning applications in network intrusion detection revealing that neural network architectures appear to be better features extractors. They also, however, noted that traditional machine learning algorithms still play a role in practice due to their more efficient computational requirements and easier implementation. Ahmed et al. also reported similar observations. Karnin et al. [19], argued that bread-and-butter classifiers are still viable

options for actual deployment settings, especially when computational resources and memory are scarce. Focus on hybrid intrusion detection architectures has gained increasing interest recently. Reinforcement learning for intrusion detection in cloud computing environment to find adaptive learning mechanisms by Jain and Paul [20]. Similarly, Vinay et al. Federated Learning Approaches for IoT Security [21] and highlighted the necessity of privacy-preserving machine learning models. According to their findings, the future of intrusion detection systems may utilize the model that takes advantage of classical machine learning algorithms and methods for distributed and collaborative learning:

Another area in which the technology (block chain) has proved to be a promising research direction for intrusion detection. Li et al. Blockchain — DOD, M. S., Fernando (2018).[22] reviewed blockchain based IDS architectures and the potential of using blockchains for threat monitoring in a decentralized, secure environment. The authors suggest that fusing machine learning with blockchain infrastructures could strengthen trust, transparency and resiliency in decentralized environments.

III. COMPARATIVE ANALYSIS

The performance of machine learning models in the context of an intrusion detection system is determined by a few aspects, namely: the emphasis placed on dataset attributes, feature selection strategies, attack diversity and resources available for feature extraction with those necessary to deploy [3].

Although positive results have come out of many studies, it is not shown that one algorithm always excels in all intrusion detection scenarios and each study reaches a conclusion about the efficiency of each algorithm. Therefore, comparative study serves as useful for best technique selection based on security environments.

Decision Tree classifier is popular for its simple implementation, interpretable results. They form simple, interpretable decision rules that can be easily understood by a security analyst, thus well suited for scenarios in which interpretability is of utmost importance. However, when the datasets are too complicated and contain several classes coming from the same type of attacks then Decision Trees are likely to get overfitted [4], [5].

Random forest has emerged to be one of the states of art traditional ML algorithms for intrustion detection. By combining multiple decision trees, it improves generalization performance and reduces the risk of overfitting.

The Random Forest classifiers have demonstrated high detection and low false positives on NSL-KDD [7], UNSW-NB15 [8]and CICIDS [9] datasets. Highers margins which allow us to train better → but more memory and compute overheads.

For classification tasks SVM (Support Vector Machines) are known to do very well even in high dimensional feature space. They are capable of determining the most accurate decision boundaries to accurately detect complicated attack patterns. Detection performance has been reported to be comparable for Random Forest models, with a much higher complexity on training however due to larger data sets [10], [11].

K-Nearest Neighbors is one of the simplest yet powerful algorithm to detect attack instances based on similarity measures. Although, it has a good performance on small datasets however when amount of training data increases its prediction time increases sharply which makes it less appropriate for real-time intrusion detection applications [13], [14].

Naïve bayes and Logistic Regression are still attractive algorithms due to their fast handling and easy implementation. The detection performance of single-stage methods is usually not as good as those from ensemble-based approaches, but they are extremely useful when fast inference speed for deployment in low-resource settings is needed [15], [17].

In conclusion, Random Forest has the best overall balanced performance of accuracy and robustness while SVM gives high classification ability. Naïve Bayes and Logistic Regression are still important because they would provide the fastest solutions of all 3 algorithms while Decision Trees is more interpretable.

It is very clear from the literature that Random Forest still occupies one of the most balanced performance metric considerations for applications in intrusion detection. While SVM shows good classification ability, it suffers from scalability issue.

Table I. Comparative Analysis of Traditional Machine Learning Algorithms for IDS

Algorithm	Detection Accuracy	Training Time	Interpretability	Computational Cost	Real-Time Suitability
Decision Tree	High	Fast	Very High	Low	High
Random Forest	Very High	Moderate	Moderate	Moderate	High
SVM	High	Slow	Low	High	Moderate
KNN	Moderate	Fast	High	High During Inference	Low
Naïve Bayes	Moderate	Very Fast	High	Very Low	Very High
Logistic Regression	Moderate	Fast	High	Low	Very High

Light-weight algorithms such as Naïve Bayes and Logistic Regression are still used when the focus is on optimized performance rather than achieving maximum detection accuracy, for instance, in production systems. All in all, to choose the algorithm to employ there should be based on operational realisations rather than solely performance metrics of classification.

IV. RESEARCH GAP

Reliance on benchmark datasets: Benchmark datasets are widely used by most IDS models, e.g., NSL-KDD, KDD Cup 99, CICIDS2017 and UNSW-NB15 but those do not reflect real-world modern cyber-attacks adequately.

Black box nature: Aalmost all high performing systems behave like a black box, where security analysts find it difficult to interpret the decisions of those systems.

Class imbalance: Unbalanced classes in IDS datasets typically lead to poor performance of the models on rare but important attack types, as normal traffic class predominates.

Evolution of cyber threats: The dynamic nature of network traffic and the availability of new attack techniques means that static trained models perform poorly over time.

Narrow evaluation: Although most studies verify model on held out data, they ignore other factors that arise when deploying, like latency, scalability or resource use.

V. CHALLENGES IN INTRUSION DETECTION SYSTEMS

Class Imbalance: Traditional IDS datasets exhibit class imbalance, with a small number of attack samples and significantly larger normal traffic compared to attack traffic. These cannot be a forwarded well into a trained model leading to shifting the focus mainly on majority classes while rare but critical attacks are ignored as they account for most of the data.

Concept Drift: Changes in network behavior and attack patterns render models trained on historical data less effective, necessitating ongoing retraining.

Adversarial Attacks: Attackers can craft imperceptible modifications to class network traffic following the same distribution resulting in a low detection accuracy and thereby causing systems to be less reliable.

Scalability - Many enterprises and cloud networks and most IoT generate huge traffic volumes, making it computationally challenging to perform real-time detection.

False Positives and False Negatives: High false positive rates tend to increased alert fatigue (i.e., security analyst gets overwhelmed by too many alerts such that important alerts may miss their attention), however, if there are false negatives then the malicious activities would stay undetected and make balancing performance a challenging task.

Interpretability and Trust: Many high performing IDS models function as black boxes, making it difficult for users to understand how decisions were made or to trust them. For practical deployment without sacrificing detection performance, explainable AI (XAI) needs to be integrated.

VI. CONCLUSION AND FUTURE SCOPE

The latest rise of digital communication, cloud computing, and IoT has come along with pushing some features of cybersecurity to the front. One such feature is Intrusion Detection Systems (IDS) [3]. Some of the machine learning techniques which have been

used to improve the IDS are-DT, RF, SVM, kNN, NB and Logistic Regression.Among these, Random Forest can provide accuracy and robustness at the same time while Naïve Bayes and Logistic Regression can still provide decent performance for resource-constrained environments. All these advances notwithstanding their real-world application are still quite limited due to class imbalance, concept drift, adversarial attacks, false alarms whose side-effects prevent a deployment of such ML systems in practice and fail either due to inability or even new domains where one does not have access to incident pairs on which the system is going be evaluated for training the system itself. Future work focuses on adaptive and scalable explainable IDS frameworks. It addresses the ways in which by combining Explainable AI (XAI), federated learning, blockchain and reinforcement learning, the system can become a more transparent, private, dependable and protective ecosystem to threats.

REFERENCES

[1] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *International Journal of Computer Networks & Communications*, vol. 8, no. 2, pp. 1–25, 2016.

[2] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective*, vol. 25, nos. 1–3, pp. 18–31, 2016.

[3] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6.

[4] M. Chandrasekaran and K. Meena, "A survey of intrusion detection techniques in computer networks," *Journal of Cyber Security Technology*, vol. 4, no. 2, pp. 105–125, 2020.

[5] B. Nancharaiah, A. Visva Sangeetha, A. Brahmareddy, R. M. Ganesh, N. Venu, and R. V. K. Reddy, "Analysis of visual communication effect of color in print advertising design based on decision tree classification algorithm," in *Proc. International Conference on Smart Technologies for Smart Nation*, 2023, pp. 804–808.

[6] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[7] C. Zhang, W. Wang, L. Liu, J. Ren, and L. Ya, "Three-branch random forest intrusion detection model," *Mathematics*, vol. 10, no. 23, Art. no. 4460, 2022.

[8] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced intrusion detection systems performance with UNSW-NB15 data analysis," *Algorithms*, vol. 17, no. 2, Art. no. 64, 2024.

[9] A. Pinto, L. Herrera, Y. Donoso, and J. Gutierrez, "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," *Sensors*, vol. 23, no. 5, Art. no. 2415, 2023.

[10] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[11] A. A. Aydin and E. Duman, "Intrusion detection systems and machine learning: A review," *IEEE Access*, vol. 9, pp. 115067–115086, 2021.

[12] A. J. A. Immastephy and K. Punitha, "A systematic review on network intrusion detection system based on machine learning and deep learning approaches," *E3S Web of Conferences*, vol. 540, Art. no. 14006, 2024.

[13] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Transactions on Information Theory*, vol. 13, no. 1, pp. 21–27, 1967.

[14] R. Sharma, S. Gupta, and P. Verma, "Intrusion detection in IoT using machine learning: A survey," *Journal of Cyber Security Research*, vol. 8, no. 4, pp. 87–104, 2020.

[15] P. Domingos and M. Pazzani, "On the optimality of the simple Bayesian classifier under zero-one loss," *Machine Learning*, vol. 29, nos. 2–3, pp. 103–130, 1997.

[16] N. V. Chawla, K. Bowyer, L. Hall, and W. Kegelmeyer, "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[17] D. W. Hosmer, S. Lemeshow, and R. Sturdivant, *Applied Logistic Regression*, 3rd ed. New York, NY, USA: Wiley, 2013.

[18] W. K. Ng, J. Tan, and M. Lee, "Network intrusion detection using deep learning: A comprehensive

survey," *Journal of Network and Computer Applications*, vol. 108, pp. 1–18, 2018.

[19] U. Ahmed, M. Nazir, A. Sarwar, T. Ali, E. M. Aggoune, T. Shahzad, and M. A. Khan, "Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering," *Scientific Reports*, vol. 15, 2025.

[20] R. Jain and S. Paul, "Q-learning-based intrusion detection in cloud computing environments," *Future Generation Computer Systems*, vol. 114, pp. 369–379, 2021.

[21] G. Vinay, S. Kumar, and A. Reddy, "Security of Internet of Things using federated learning and deep learning: Recent advancements, issues and prospects," *ICT Express*, vol. 9, pp. 941–960, 2024.

[22] J. Li, X. Wang, and H. Zhao, "Blockchain-based intrusion detection system for IoT: A survey," *IEEE Access*, vol. 8, pp. 156412–156426, 2020.

[23] M. Zhou, Y. Wang, and Z. Liu, "Lightweight secure communication protocols for Internet of Things environments," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 45–56, 2019.

[24] M. Sethi and V. Verma, "Improving intrusion detection systems using reinforcement learning: Responding to new cyber-attacks and threats," in *Proc. International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, 2025, pp. 1–6.

[25] M. Zhou, Y. Zhang, and J. Liu, "A hybrid reinforcement learning model for intrusion detection in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10231–10239, 2019.