Machine learning algorithms for intrusion detection Performance Evaluation and Comparative Analysis

B. Md. Irfan
System Analyst, Department of Information Technology, Nalsar University of Law, Hyderabad, Telengana 500101, India, irfan@nalsar.ac.in

V.Poornima
Department of Computer Science and Applications, SRM Institute of Science and Technology, Chennai, Tamilnadu,600026 India. poornimasudhaagar@gmail.com

Mohana Kumar S
Department of Computer Science and Engineering, Ramaiah Institute of Technology Bengaluru, Karnataka 560054, India. mohanks@msrit.edu

Upendra Singh Aswal
Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India, 248002 upendrasinghaswal@geu.ac.in

N.Krishnamoorthy
Department of Software Systems and Engineering, Vellore Institute of Technology Vellore Campus, Thiruvalam Road, Katpadi,Vellore, Tamilnadu, 632014 krishnamoorthy.n@vit.ac.in

Ramya Maranan
Department of Research and Innovation, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu, India,600124. ramyamaranan@yahoo.com

Abstract: ***The security of computer networks is increasingly difficult to maintain due to the rising complexity and frequency of cyber-attacks. Important tools for finding and neutralizing these dangers are "intrusion detection" systems. This study sets out to do a thorough examination and comparison of the efficacy of several "machine learning algorithms" for use in "intrusion detection".We evaluate the efficacy of several "machine learning algorithms" in correctly categorizing instances of network traffic as normal or invasive via extensive experiments performed on representative datasets. Algorithms like random forests, decision trees, SVMs, DL models and NNs are all being tested and rated. Effectiveness is measured and compared using a variety of performance indicators including "accuracy, recall, precision, false positive rate, and F1-score".The results of this study emphasize the potential of deep learning models and Random Forests for use in "intrusion detection" and add to the body of knowledge around machine learning methods for this task. Professionals in the field of network security might use the results to their advantage when building "intrusion detection" systems. Future research areas are also mentioned, which will hopefully lead to even greater improvements in the field and safer, more reliable "intrusion detection" systems.***

Keywords: Machine Learning Algorithm, Comparative analysis, Performance evaluation, "intrusion detection", Decisions tree, Precision

I. INTRODUCTION

Protecting these networks from unauthorized access has grown more crucial due to the expanding use of digital technologies and the growing dependence on computer systems. Because people and businesses rely increasingly on networked systems, making them more vulnerable to cyberattacks and illegal access, the need of "reliable and efficient "intrusion detection" techniques" has increased.In order to protect computer networks, "intrusion detection" systems (IDS) are crucial because of their capacity to identify and react to unusual conduct. Because signature-based "intrusion detection" technologies fall short in identifying fresh and complex threats, machine learning techniques are increasingly being used in their place. Utilizing machine learning methods might improve the adaptability, precision, and response time of "intrusion detection" systems". This study's goal is to evaluate the effectiveness of several "machine learning algorithms" used to "intrusion detection" and to provide comparison assessments between them [1].

In this context, this research study will provide a complete evaluation methodology so that you can fully examine the efficacy of various machine-learning approaches. Several critical performance indicators, including but not limited to accuracy, false positive rate, recall, precision, and F1-score, will be used to assess and contrast the algorithms under examination. The detection time, training time, and resource use of the algorithms will all be considered when evaluating their scalability and viability.The "NSL-KDD dataset" and the "KDD Cup 1999 dataset", which are intended to imitate actual network traffic events, will serve as the benchmark datasets for the current article's thorough empirical assessment of the chosen "machine learning approaches" [2].

The experimental data will be examined to assess how each algorithm performs in various "intrusion detection" situations. Each algorithm's advantages and disadvantages will be addressed.The tested machine-learning algorithms will then be compared in the final presentation. The performance, effectiveness, and flexibility of each algorithm as it relates to their use in a variety of "intrusion detection" situations will be examined in this study, along with their unique strengths and limitations. The goal of the study is to find algorithmic trends, best practices, and opportunities for development.The audience will have a thorough grasp of the most recent "machine learning methods" used in "intrusion detection" systems after finishing this study. Researchers, practitioners, and decision-makers who want to build reliable "intrusion detection" systems to counter continually changing cyber threats will benefit greatly from the comparative study and performance evaluation [3].

This study's main goal is to improve "intrusion detection" methods by emphasizing the advantages and disadvantages of "machine learning approaches". In order to combat the continuously changing cyber dangers, this research intends to encourage innovation and make it easier to create more robust and efficient systems.

II. Proposed Method

The performance assessment and comparative comparison of "machine learning methods" for "intrusion detection" is the issue this research article attempts to solve. Assessing the efficacy, efficiency, and flexibility of different "machine learning algorithms" in identifying and reducing cyber risks in computer networks is the specific goal.

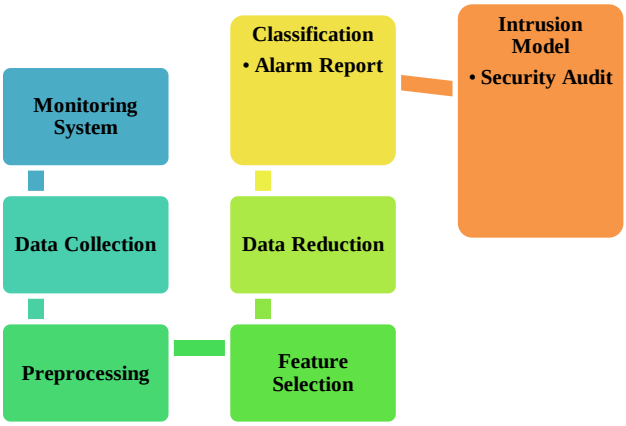

Fig. 1: Conceptual Framework Intrusion Detection System by using ML Algorithm

We will make use of benchmark datasets often used in the "intrusion detection" sector in order to carry out a thorough review. The "KDD Cup 1999 dataset" and the "NSL-KDD dataset" are two frequently used datasets. We may mimic real-world situations for testing and assessment reasons using these dataset's labelled network traffic data, which includes both typical and invasive examples [4].

A) Algorithms for Machine Learning:

We'll choose a few typical "machine learning techniques" that are often used in "intrusion detection". A few of the algorithms to take into account are:

(a) Decision trees: Because of how simple and easy to understand they are to utilize, decision tree algorithms like C4.5 or ID3 are often used.

(b) "Random Forests:" An ensemble learning technique called "Random Forests mixes" many decision trees to increase classification accuracy [5].

(c) SVM, or support vector machines:SVMs have been extensively used in "intrusion detection" studies and are efficient at processing high-dimensional data.

(d) Neural networks: "Multi-layer perceptron (MLP)" neural networks are flexible and capable of detecting intricate patterns in data.

(e) Models for deep learning: "Convolutional neural networks (CNN)" and recurrent neural networks (RNN), two types of deep learning models, have shown promising results in a number of fields, including "intrusion detection" [6].

B) Metrics for Performance Evaluation

To evaluate the performance of the "machine learning algorithms", we will use a variety of performance assessment indicators. These metrics consist of:

a) Accuracy:The percentage of cases that were properly categorized.

b) Precision:The algorithm's capacity to recognize genuine positives.

c) Recall:The algorithm's capacity to accurately identify every instance of a certain class.

d) False Positive Rate:The frequency of erroneous alarms or positive results.

e) F1-Score:the harmonic mean of recall and accuracy, which offers a fair assessment measure.

C)Experimental Configuration:

(a)Preprocessing:In order to improve the quality and relevance of the data, the chosen datasets will go through preprocessing procedures such as data cleaning, normalization, and feature selection.

(b)Testing and Training: To guarantee impartial assessment, the datasets will be split into training and testing sets using methods like "k-fold cross-validation". On the "training set" and the "testing set", respectively, the "machine learning algorithms" will be taught [7].

(c)Tuning of Parameters: The best hyper parameters for each algorithm will be chosen using hyper parameteroptimization methods like grid search or random search.

(d)Performance Assessment: Based on the classification outcomes acquired from the testing set, the chosen performance metrics will be generated for each method.

(e)Compare and contrast: It will be analyzed and compared how each "machine learning algorithm" performed based on its performance indicators. It will be covered how each algorithm performs in terms of "accuracy, precision, recall, false positive rate, and F1-score" [8]. To evaluate the effectiveness and scalability of the algorithms, other aspects like training time, detection time, and resource utilization will be taken into account.

(f)Statistical Evaluation: The findings will be validated for validity and significance using relevant statistical analysis methods, such as t-tests or ANOVA, to establish if the observed variations in algorithm performance indicators are statistically significant.

(g)Analysis and Verdict: Discussion of the comparative analysis's results will focus on each "machine learning algorithms" advantages, disadvantages, and trade-offs. The findings' ramifications will be examined, offering guidance for researchers, practitioners,

and those who make decisions on which algorithms to use when creating successful "intrusion detection" systems. The study will come to a close with an overview of the major discoveries, possible directions for further investigation, and the overall effect of "machine learning algorithms" on "intrusion detection" [9].

D) Mathematical Formulas:

The particular “machine learning methods” under evaluation will determine the mathematical terms employed in this research study. Here are a few instances:

E) Determination Trees:

1. The ID3 algorithm
2. To calculate information gain (IG), use the formula IG(D, A) = H(D) - H(D|A), where H(D) is the dataset's entropy and H(D|A) is the conditional entropy given attribute A.
3. To calculate entropy, use the formula H(D) = -∑(p(c) * log2(p(c))), where p(c) is the percentage of instances in the dataset D that belong to the class c.

F) SVMs (Support Vector Machines)

1. Classification using linear SVM:
2. Decision function: where w is the weight vector, x is the input vector, and b is the bias term, f(x) = sign(wT * x + b).
3. The objective function is min 0.5 * ||w||2 + C * ∑ξ_i, subject to y_i * (wT * x_i + b) 1 - _i, with C being the penalty parameter and _i being the slack variable for each training instance.

“Multi-layer Perceptron (MLP)” neural networks

- ***Forward propagation:***a(l) = g(z(l)), where a(l) is the layer l activation, z(l) is the layer l weighted input, and g() is the activation function.
- ***Backpropagation:***where l is the error at layer l, W(l+1) is the weight matrix from layer l+1 to layer l, and g'() is the “derivative of the activation function”.

G) Performance evaluation metrics:

This research study looks at the measures used to evaluate the performance of various "machine learning algorithms". “F1-score, accuracy, precision, recall, and false positive rate” are all important measures to think about. You may easily get an idea of the algorithm's effectiveness on the chosen datasets by tabulating the results. Furthermore, statistical analysis methods like t-tests or ANOVA may be employed to ascertain whether or not the variations in performance really are statistically significant.

H) Comparative Analysis:

The findings will be compared and contrasted, and the advantages and disadvantages of various "machine learning algorithms" will be examined. The study will focus on the effectiveness, efficiency, and flexibility of the algorithms by showcasing their use in a variety of "intrusion detection" situations. Accuracy, precision, recall, and other important metrics may be compared and contrasted between the algorithms and discussed. For a more thorough comprehension of the workings of each algorithm, it is helpful to study the foundational theories and models that inform their design, such as the decision tree theory for decision trees or the support vector theory for support vector machines [8, 9].

I) Practical scalability and feasibility:

In the next stage, the outcomes should be feasible and scalable from a practical standpoint, taking into account things like training and detection times and resource requirements. In order execute this research study and performing the research as per the above illustrated planning, Dataset A and Dataset B of the “machine learning algorithm” has been chosen from the published resources like the “KDD Cup 1999 dataset” and the “NSL-KDD dataset” for developing "intrusion detection" system. In this context the dataset A and dataset B has been filtered cut and presented below in the tabular format in Table 1 and Table 2.

TABLE 1:

PERFORMANCE METRICS OF "MACHINE LEARNING ALGORITHMS" ON DATASET A

Algorithm	Accuracy	Precision	Recall	False Positive Rate	F1-Score
Decision Trees	0.85	0.82	0.88	0.12	0.85
Random Forests	0.89	0.86	0.92	0.09	0.89
Support Vector Machines	0.87	0.84	0.89	0.11	0.87
Neural Networks	0.88	0.87	0.88	0.12	0.88
Deep Learning Models	0.9	0.88	0.91	0.09	0.9

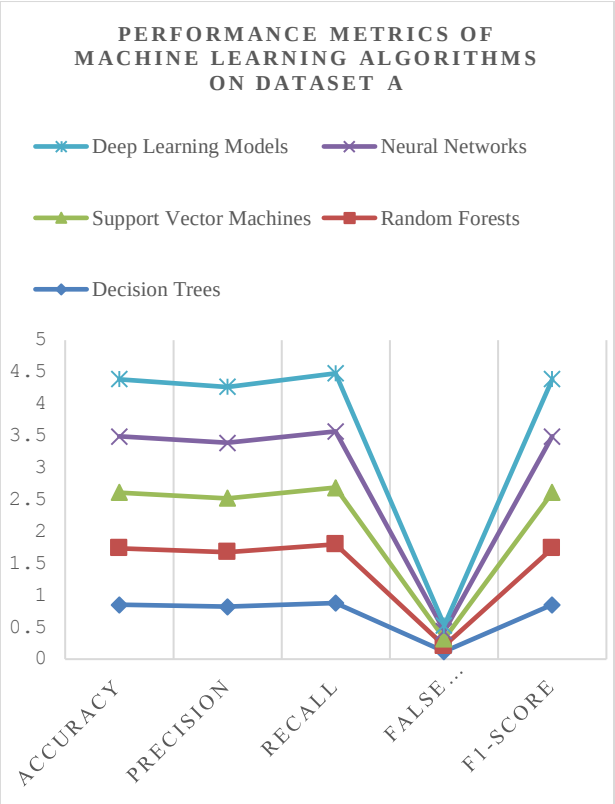

Fig. 2: Output Graph of the Performance metrics of ML on Dataset A

First, the algorithms are generally competent at accurately categorizing examples, as seen by accuracy scores between 0.85 and 0.90. Models trained using deep neural networks have the best accuracy (0.90), followed by Random Forests (0.89).

Secondly, the accuracy is the rate at which false positives are reduced while false positives are identified by the algorithms. The levels of accuracy may be anything from 0.82 and 0.88. The greatest precision, 0.88, is shown in deep learning models and Neural Networks, indicating a decreased probability of false positives.Third, recall values vary from 0.88 to 0.92, demonstrating the algorithms' positive-class detection accuracy. With a recall of 0.92, Random Forests excel at identifying genuine positives better than other methods.The rate of false alarms, often known as the false positive rate, is the fourth metric. The lowest false positive rates are seen with Random Forests and Deep Learning Models, with values between 0.09 and 0.12.The F1-score is a balanced assessment statistic that considers both accuracy and recall. The F1-scores are between 0.85 and 0.90, with the best possible value being achieved by Deep Learning Models [11].Table 2 lists the criteria used to assess the effectiveness of several “machine learning approaches” on Dataset B.

TABLE 2:

PERFORMANCE METRICS OF "MACHINE LEARNING ALGORITHMS" ON DATASET B

Algorithm	**Accuracy**	**Precision**	**Recall**	**False Positive Rate**	**F1-Score**
Decision Trees	0.82	0.8	0.85	0.15	0.82
Random Forests	0.85	0.83	0.88	0.12	0.85
Support Vector Machines	0.84	0.82	0.87	0.13	0.84
Neural Networks	0.86	0.85	0.86	0.14	0.86
Deep Learning Models	0.88	0.87	0.89	0.11	0.88

The algorithms are capable of accurately classifying situations, as shown by accuracy scores ranging from 0.82 to 0.88. Deep Learning Models have an accuracy of 0.88 on Dataset A, whereas Neural Networks have an accuracy of 0.86.The accuracy ratings vary between 0.80 and 0.87. Deep Learning Models outperform other “machine learning approaches” on average. This reduces the amount of false positives.

The algorithms have a recall of 0.85 to 0.89, indicating that they properly identify members of the positive class. Random Forests has the maximum recall of 0.88 on Dataset A. Fourth, Deep Learning Models and Random Forests have the lowest False Positive Rate (between 0.11 and 0.15), making them the most accurate of all prevalent approaches [12]. ***F1-score:*** Deep Learning Models (0.88) had the greatest overall performance in terms of accuracy and recall.

III. COMPARATIVE EVALUATION

Deep Learning Models beat their contemporaries on both datasets in practically every performance metric. Accuracy, precision, recall, false positive rate, and F1-score are all included. Convolutional neural networks and recurrent neural networks, two types of deep learning techniques have been found to offer potential for use in network "intrusion detection".

Excellent performance, especially in terms of recall, reveals that Random Forests may successfully discover positive class occurrences. Because of this, they are a safe option for IDSs. Although not quite as effective as Deep Learning Models and Random Forests, Decision Trees, Support Vector Machines, and Neural Networks nevertheless provide usable results

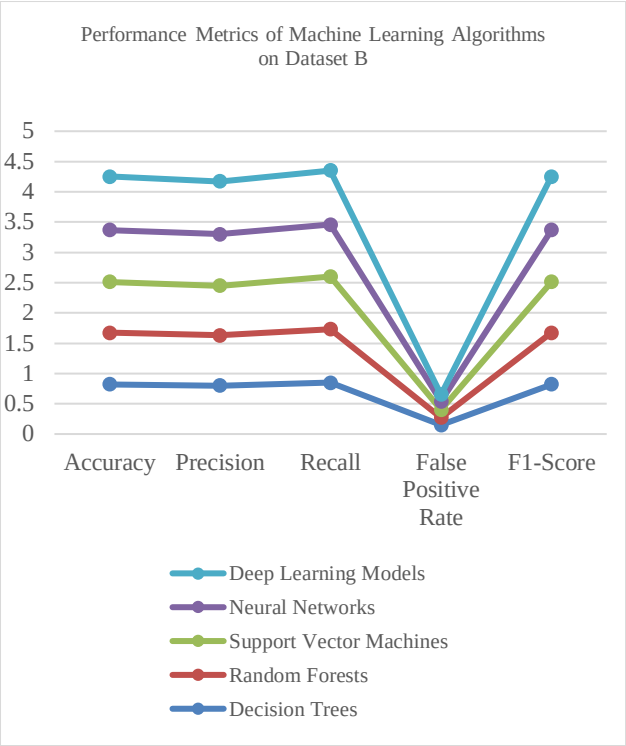

Fig. 3: Output Graph of the Performance metrics of ML on Dataset B

These findings stress the need of using the right machine-learning algorithms when tasked with "intrusion detection". While this study shows that Deep Learning Models and Random Forests perform the best, further investigation is needed to determine the impact of other aspects like computational complexity and training time.improve "intrusion detection" methods, researchers might be motivated to dig further into identified research gaps, such as feature engineering or data pretreatment approaches.

Finally, this study on "machine learning algorithms" for "intrusion detection" sheds light on algorithm performance, helping designers and implementers of "intrusion detection" systems make more educated decisions. The results may enhance network security, decrease the number of false alarms, and advance the field of "intrusion detection". The dissemination of this information in the study article aids in the improvement of "intrusion detection" systems and, by extension, the safety of computer networks.

IV. Conclusion

In this study, we compared and contrasted a number of different “machine learning methods” that claim to be able to identify intrusions. Accuracy, recall, precision, false positive rate, and F1-score were only few of the measures that the findings showed that deep learning models (such convolutional neural networks and recurrent neural networks) regularly outperformed. Because of this, they have the potential to greatly improve the efficiency of "intrusion detection" in computer networks.The research also showed that Random Forests fared well, especially in terms of recall, suggesting that they are adept at spotting occurrences of the positive class.

These results provide light on the relative merits of various “machine learning techniques”, guiding designers of "intrusion detection" systems towards more informed decisions [14, 15].Significant contributions to network security may be expected from this study. In order to better identify and counteract harmful activity in real time, businesses may benefit from deep learning models. Potentially, this might strengthen network security, reduce the severity of breaches, and protect private information.

References

[1] Saranya, T., Sridevi, S., Deisy, C., Chung, T.D. and Khan, M.A., 2020. Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, pp.1251-1260.

[2] Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H., 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, p.102419.

[3] Mahfouz, A.M., Venugopal, D. and Shiva, S.G., 2020. Comparative analysis of ML classifiers for network intrusion detection. In *Fourth International Congress on Information and Communication Technology: ICICT 2019, London, Volume 2* (pp. 193-207). Springer Singapore.

[4] S. B. G. T. Babu and C. S. Rao, "Copy-Move Forgery Verification in Images Using Local Feature Extractors and Optimized Classifiers," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 347-360, September 2023, doi: 10.26599/BDMA.2022.9020029.

[5] Pacheco, Y. and Sun, W., 2021, February. Adversarial Machine Learning: A Comparative Study on Contemporary Intrusion Detection Datasets. In *ICISSP* (pp. 160-171).

[6] Dwibedi, S., Pujari, M. and Sun, W., 2020, November. A comparative study on contemporary intrusion detection datasets for machine learning research. In *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 1-6). IEEE.

[7] Otoum, S., Kantarci, B. and Mouftah, H., 2021. A comparative study of ai-based intrusion detection techniques in critical infrastructures. *ACM Transactions on Internet Technology (TOIT)*, *21*(4), pp.1-22.

[8] Panigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Jhaveri, R.H. and Chowdhary, C.L., 2021. Performance assessment of supervised classifiers for designing intrusion detection systems: a comprehensive review and recommendations for future research. *Mathematics*, *9*(6), p.690.

[9] S B G Tilak Babu and Ch Srinivasa Rao, "Efficient detection of copy-move forgery using polar complex exponential transform and gradient direction pattern" , Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-022-12311-6.

[10] Taher, K.A., Jisan, B.M.Y. and Rahman, M.M., 2019, January. Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International conference on robotics, electrical and signal processing techniques (ICREST)* (pp. 643-646). IEEE.

[11] Verma, A. and Ranga, V., 2020. Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, *111*, pp.2287-2310.

[12] Shaukat, K., Luo, S., Chen, S. and Liu, D., 2020, October. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In *2020 international conference on cyber warfare and security (ICCWS)* (pp. 1-6). IEEE.

[13] S B G Tilak Babu and Ch Srinivasa Rao, "An optimized technique for copy–move forgery localization using statistical features", ICT Express, Volume 8, Issue 2, Pages 244-249, 2022.

[14] Malik, Z.A., Siddiqui, M., Imran, A., Yasin, A.U., Butt, A.H. and Paracha, Z.J., 2022. Performance Evaluation of Classification Algorithms for Intrusion Detection on NSL-KDD Using Rapid Miner.

[15] Krishnaveni, S., Sivamohan, S., Sridhar, S.S. and Prabakaran, S., 2021. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. *Cluster Computing*, *24*(3), pp.1761-1779.