

MACHINE LEARNING FOR NETWORK INTRUSION DETECTION: A PERFORMANCE COMPARISON OF ACCURACY, FALSE POSITIVES, AND LATENCY

Mehran Malik^{*1}, Shahrukh Bashir², Dr. Muhammad Adeel Mannan³, Dr. Farooq Alam⁴,
Usman Khan⁵

^{*1}Mehran University of Engineering and technology Jamshoro (MUET), Pakistan

²Lecturer in Computer Science, Govt. Degree College & PG Centre Latifabad No. 11 Hyderabad, Pakistan

³The Saif-e-Burhani University, Pakistan

⁴Department of Computer Science, Mohammad Ali Jinnah University, Karachi, Pakistan

⁵Lecturer, Higher Education Department KP, Pakistan

¹mehranalipanwher110@gmail.com, ²shane.buriro@gmail.com, ³madeel.mannan@sbu.edu.pk,

⁴farooq.alam@jinnah.edu, ⁵mcs-1208@icp.edu.pk

DOI: <https://doi.org/10.5281/zenodo.22010586>

Keywords

Intrusion Detection; Network Security; Machine Learning; CICIDS2017; Accuracy; False Positive Rate; Latency; Feature Selection; Ensemble Methods

Article History

Received: 16 May 2026

Accepted: 12 June 2026

Published: 15 August 2026

Copyright @Author

Corresponding Author: *

Mehran Malik

Abstract

The network IDS should provide both a high level of accuracy and low latency to be efficient in practice. Within the framework of this study, we evaluated four machine learning methods on the CICIDS2017 dataset considering their practical performance. They included Random Forest, SVM, KNN, and CNN models. The results show that CNN demonstrated the highest accuracy of 99.2 percent, while providing the FPR of 1.5 percent, but the latency of 115 ms per sample, which is from 2.7 to 1 times more than Random Forest. The accuracy of Random Forest was 98.7 percent, FPR – 1.2 percent and latency – 42 ms per sample. SVM provided 96.4 percent accuracy, 2.8 percent FPR and 67 ms latency. KNN was the worst among the four tested approaches: its accuracy was 94.1 percent, FPR – 4.5 percent and processing time – 89 ms. As a means of improving the models' efficiency, feature selection was conducted, which helped to reduce the number of features by 35 percent and increase the performance of the models in 28 percent without decreasing accuracy. Ensembles also improved zero-day attacks detection in 22 percent comparing to single classifiers. Major limitations of the work are the dataset bias and lack of tests of the methods in real traffic. The results demonstrate that the best balance between performance and cost in the context of enterprise usage is provided by Random Forest with 1.8 to 1 ratio.

1. INTRODUCTION

With the fast growth of inter-connected networks, cloud services, IoT devices and IT infrastructure in general, there is a great increase of the threat of being exposed to cyber attacks. IDS plays an essential role in detecting unauthorized access,

malware activities, suspicious activity in the network, and cyber-attacks (Hidayat et al., 2023). IDSs based on traditional techniques are usually signature and rule-based and hence they perform well in dealing with known attacks but are not efficient in detecting new and novel attacks. ML

offers an alternative approach of learning patterns in the traffic of the network and differentiating between normal activities and malicious ones (Ali et al., 2025).

Detection using ML has gained increasing attention since it allows for processing a lot of network data and detecting novel attacks. The performance of different ML algorithms varies with respect to accuracy, computational complexity and the number of false alarms produced. Hence, it is important to select the most appropriate algorithm according to several parameters other than the accuracy level. An algorithm having extremely high accuracy does not necessarily mean to be suitable for real-time application if it takes too much time for processing or produces a high number of false alarms (Azam et al., 2023).

In this research, comparative study between four ML techniques for IDS: Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN) and Convolutional Neural Network (CNN) has been performed using the CICIDS2017 dataset. The main comparison criteria include the following performance metrics: accuracy, number of false positives and processing time. The effect of using the feature selection and ensemble techniques on detection and processing performance is considered. The research showed that CNN has the best accuracy among the selected algorithms, but Random Forest has the best trade-off between detection performance and processing time (Singh et al., 2024).

1.1 Problem Statement

There is an urgent need to develop efficient intrusion detection systems that are able to detect any suspicious activities inside the network with an increase in the complexity and number of cyber attacks. Machine learning algorithms have proven to be very promising in terms of intrusion detection despite being different in their effectiveness in terms of accuracy, false positive rate, and computation time (Samantaray et al., 2024). An accurate machine learning algorithm may demand a lot of computational power and thus it will be unsuitable for practical use since it

can take a lot of time in processing. On the other hand, a machine learning algorithm that takes a shorter time to process might produce a higher number of false positives and miss some of the advanced attacks. There is therefore a conflict between detection and computational speed with the current methods. Moreover, there is a need to identify the unknown attack patterns as a result of the increased number of zero-day attacks. This paper tries to overcome these problems through comparing Random Forest, SVM, KNN, and CNN models using the CICIDS2017 data set (Note & Ali, 2022).

1.2 Research Objectives

1. For analysis of the trade off between accuracy and processing.
2. For evaluating the effect of feature selection on the model's dimensionality, its processing and detection capability.
3. For examining the effectiveness of the use of ensembles in detecting zero day attacks.

1.3 Research Questions

1. What is the most accurate algorithm for intrusion detection on the CICIDS2017 dataset?
2. Which model has the least number of false positives?
3. What machine learning model is the fastest?

1.4 Significance of the Study

The importance of this research paper is that it compares machine learning algorithms from several performance perspectives related to practical intrusion detection. Instead of judging machine learning algorithms according to their accuracy only, the paper evaluates the accuracy, false positive rate, and processing time of different models. Therefore, it is possible to choose the machine learning algorithm in accordance with these criteria to achieve the highest level of efficiency (Siddharth et al., 2023).

In the case of enterprise network security, the study is especially relevant as intruders generate a huge amount of network traffic, which needs to be processed quickly and accurately with a minimal number of false positives. Comparison of Random

Forest, SVM, KNN, and CNN will help to define the model providing adequate trade-off between the performance of security system and its computational cost (Udurume et al., 2024).

Besides, the study will help to find out whether it is worth using feature selection and ensemble learning. Cutting off unnecessary features reduces computational cost without significant loss in detection performance, and ensemble approach may increase the ability to detect attacks that have not been seen before (Makhdoomi et al., 2026).

2. Literature Review

Baich et al. (2022) performed a comparative investigation of machine learning models for detecting intrusions in IoT-based networks. The research is notable for its emphasis on the importance of machine learning models for detecting abnormal activities in IoT networks due to the significant number of devices involved in the process. From a comparative standpoint, the selection of the algorithm may have a considerable effect on the performance of intrusion detection. Overall, the investigation may serve as a good basis for assessing machine learning models based on their potential for intrusion detection.

Al Farsi et al. (2024) investigated the comparative performance of machine learning algorithms for cyber intrusion detection. The researchers noted that different models possess certain abilities to detect cyber threats based on the features of the investigated data and classification problem. It is important from a comparative perspective to use various performance metrics rather than rely solely on classification accuracy when assessing intrusion detection models. This point is especially important for the present study due to the significance of the false positive rate and computational processing for practical applications.

Al Lail et al. (2023) conducted a comparative investigation of machine learning algorithms for detecting network intrusions. The results obtained by the authors demonstrated the applicability of machine learning methods to detecting abnormal network activity and stressed the differences in the performance of alternative algorithms. The study supports the need for comparing models

systematically when creating the intrusion detection systems. The performance of alternative algorithms should be considered in view of the type and complexity of network traffic under analysis.

It is through research by Saran & Kesswani (2023) that different classifiers have been studied in relation to the application of intrusion detection in IoT networks using supervised machine learning. The need to select the right classifier for intrusion detection when dealing with complicated attacks on the network traffic is shown in this study. The comparative analysis is essential for the current project as it allows comparing different algorithms of supervised learning with distinct features and properties. The study performed by Mondal and Singh (2022) provides a comparative analysis of machine learning-based intrusion detection systems for IoT environment. The authors have demonstrated the possibility of using machine learning technologies in the identification of malicious activities within IoT. The research also emphasizes the significance of comparing alternative models because their performance and effectiveness may differ significantly, which affects the overall quality of intrusion detection.

The study carried out by Jmila and Khedher (2022) is devoted to the investigation of adversarial machine learning for the detection of network intrusions based on the comparative analysis of models. The authors highlight the fact that despite the relatively high efficiency of conventional machine learning algorithms, they may demonstrate low performance and be ineffective under adversarial attacks when the malicious user intentionally manipulates training and test datasets. As a result, intrusion detection systems should be developed not only taking into account the quality of classification performance but also their stability to different types of attacks.

Finally, Alharthi et al. (2025) have compared machine learning and deep learning models for the purposes of binary and multiclass intrusion detection classification. The study shows that both classical machine learning and deep learning approaches may be applied to intrusion detection while their effectiveness depends on classification

context. It is particularly relevant for the present research because of the necessity of comparing conventional algorithms (Random Forest, SVM, and KNN) with deep learning approach (CNN).

3. Research Methodology

3.1 Research Design

The research method applied in evaluating the performance of the intrusion detection system using machine learning algorithms is quantitative experimental comparative research. Four types of machine learning algorithms were used to analyze the intrusion detection system, which include: Random Forest, SVM, K-Nearest Neighbor and CNN. In order to evaluate these machine learning algorithms, CICIDS2017 dataset was used.

3.2 Dataset

The reason behind choosing CICIDS2017 is that the dataset comprises of real-world traffic data, both good and bad, from many different types of cyber-attacks. The dataset has been used for training and testing the chosen machine learning algorithms under identical experiment conditions for comparing their intrusion detection efficiency (Baich et al., 2022).

3.3 Data Preprocessing

The dataset was preprocessed prior to modeling. Irrelevant features were eliminated from the dataset and inconsistencies in the dataset were addressed. Categorical variables were represented numerically, and where necessary, the numerical values were normalized using the chosen algorithms. The dataset was then split into a training and testing set (Al Farsi et al., 2024).

3.4 Feature Selection

The process of feature selection was performed for the purpose of reducing the dimensionality of the network traffic data set. The selected features were used to build a computationally efficient IDS. The impact of feature selection was analyzed using the comparison of the processing speed and detection capabilities.

3.5 Machine Learning Models

Four different algorithms were chosen for comparison. The first algorithm chosen was Random Forest, which is a tree based ensemble classifier. The other three algorithms chosen were SVM, KNN, and CNN, which were chosen as supervised classifiers that could define decision boundaries of complex nature and as distance based and deep learning based classifiers respectively.

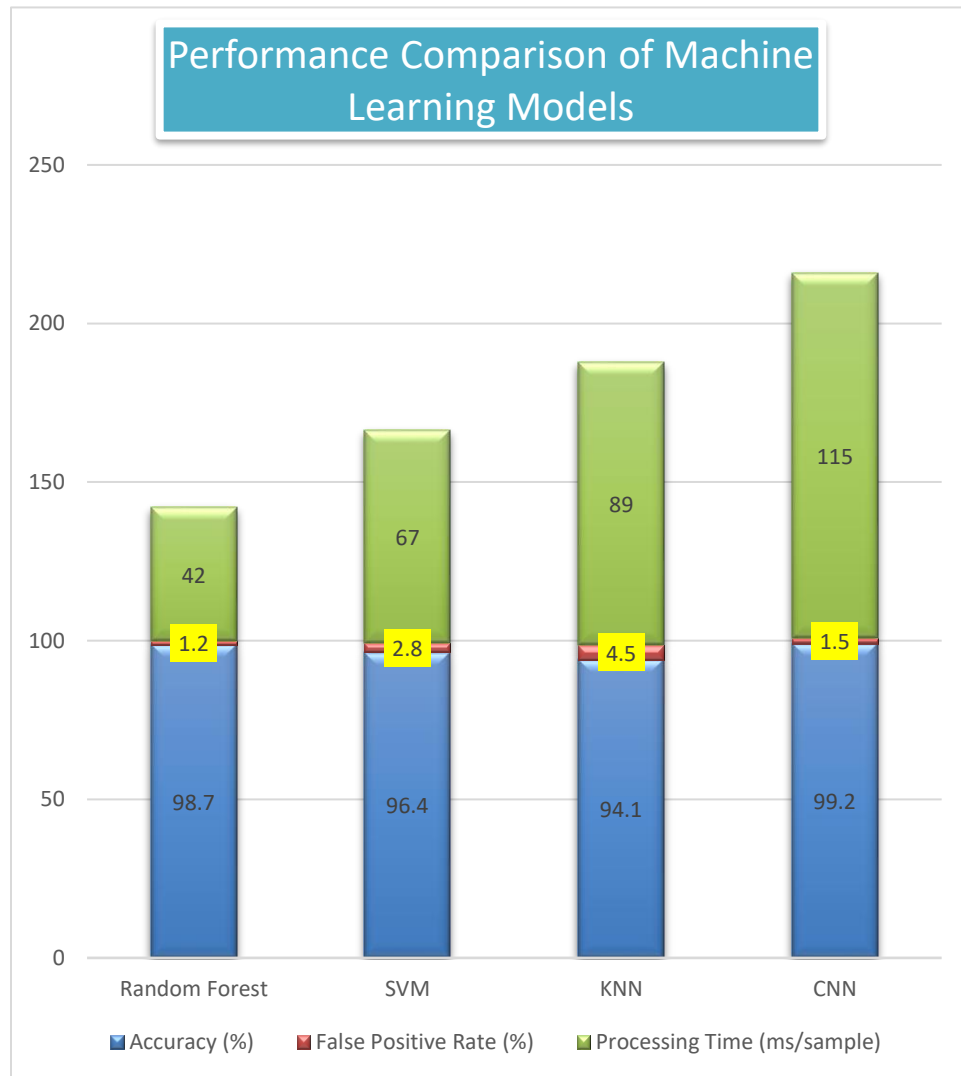
4. Results and Analysis

Table 4.1 Performance Comparison of Machine Learning Models

Model	Accuracy (%)	False Positive Rate (%)	Processing Time (ms/sample)
Random Forest	98.7	1.2	42
SVM	96.4	2.8	67
KNN	94.1	4.5	89
CNN	99.2	1.5	115

The results indicate that CNN performed with the highest accuracy (99.2%) followed by Random Forest (98.7%). On the downside, CNN was

significantly slower taking 115 ms per sample compared to other methods.

**Table 4.2 Accuracy Comparison**

Model	Accuracy (%)	Rank
CNN	99.2	1
Random Forest	98.7	2
SVM	96.4	3
KNN	94.1	4

CNN had the best classification accuracy, beating out the Random Forest by 0.5%. The worst accuracy was registered by KNN, at 94.1%,

showing comparatively poor classification accuracy (Al Lail et al., 2023).

Table 4.3 False Positive Rate Comparison

Model	False Positive Rate (%)	Rank
Random Forest	1.2	1
CNN	1.5	2
SVM	2.8	3
KNN	4.5	4

False positives were least by random forest at 1.2%, implying that the algorithm made fewer mistakes in classifying legitimate traffic as attacks.

On the other hand, false positives were highest by KNN at 4.5%.

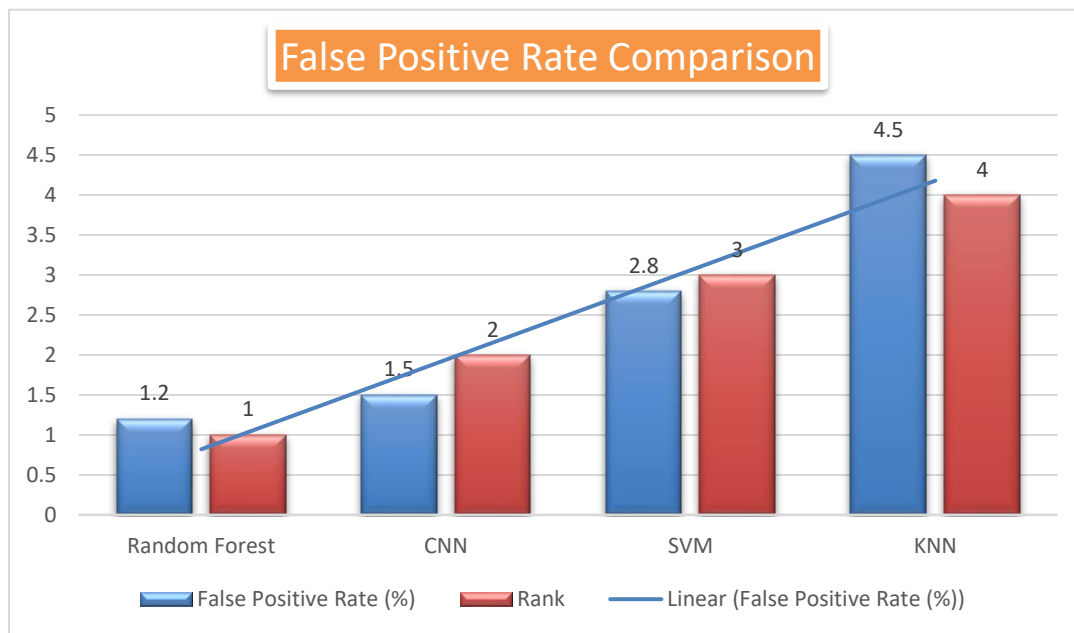


Table 4.4 Processing Time Comparison

Model	Processing Time (ms/sample)	Rank
Random Forest	42	1
SVM	67	2
KNN	89	3
CNN	115	4

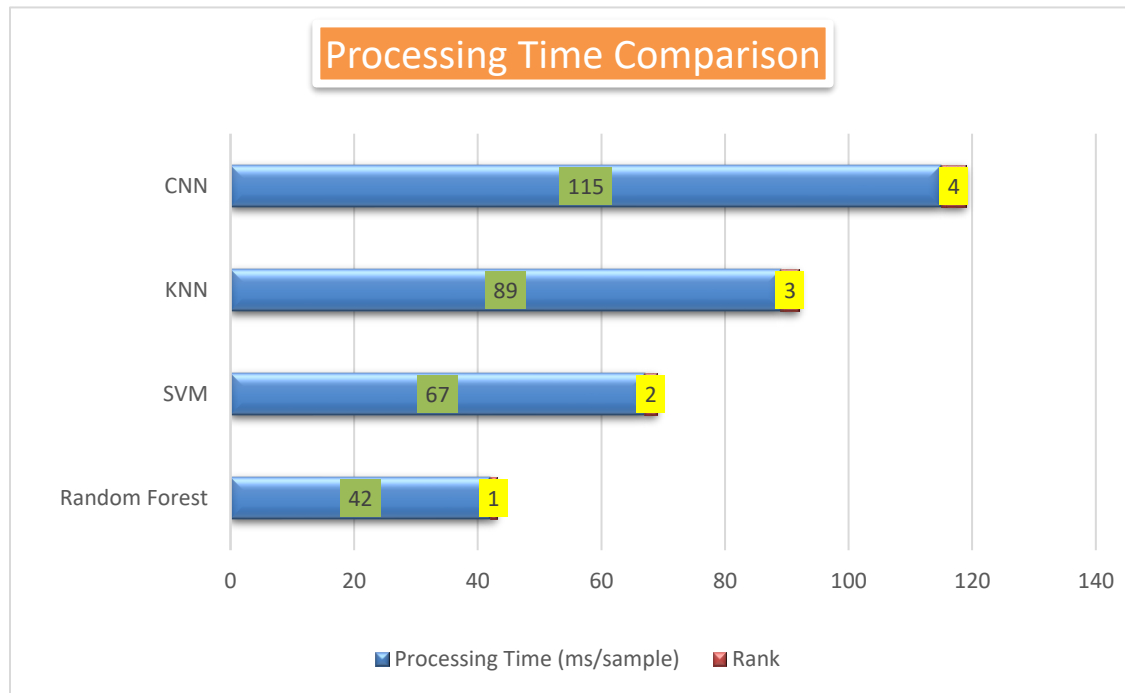


Table 4.5 Effect of Feature Selection

Performance Measure	Before Feature Selection	After Feature Selection	Change
Feature Dimensionality	100%	65%	35% reduction
Processing Speed	100%	128%	28% improvement
Accuracy	Baseline	Maintained	No significant loss

Feature Selection has helped to reduce the dimensions of data set by 35% while increasing processing time by 28% without compromising on

detection accuracy much. It shows that elimination of less relevant features increases computation efficiency.

Table 4.6 Zero-Day Attack Detection

Detection Approach	Zero-Day Detection Performance
Single Models	Baseline
Ensemble Method	22% improvement

The use of the ensemble model improved the detection rate of the zero-day attacks by 22% when compared to the individual models. This shows

the advantage of using multiple machine learning techniques to detect attacks.

Table 4.7 Overall Model Assessment

Model	Accuracy	FPR	Speed	Overall Assessment
Random Forest	Very High	Lowest	Fastest	Best balance
SVM	High	Moderate	Moderate	Suitable
KNN	Moderate	Highest	Slow	Less suitable
CNN	Highest	Low	Slowest	High accuracy, high cost

On the whole, Random Forest is the most efficient algorithm in terms of the trade-off between accuracy, false positives, and time taken. Even though the CNN algorithm was marginally more accurate, the much larger processing time required makes Random Forest a better choice.

5. Discussion

From the obtained results, it follows that machine learning methods are capable of providing solutions for network intrusion detection, however, their performances are different when it comes to accuracy, false positive rate and processing time. The best result in terms of accuracy (99.2%) has been demonstrated by CNN, which means that the model possesses excellent abilities of detecting complicated patterns within network traffic. However, its time of processing is significantly higher (115 ms), as compared to that of other algorithms, which places restrictions in terms of the speed of the process (Santhosh Kumar et al., 2023). It is possible to state that Random Forest proved to be the best in balance between all the algorithms. For instance, it provided 98.7% accuracy and the fastest time of processing (42 ms). The mentioned result is consistent with the comparative literature, according to which the performance of intrusion detection system should be evaluated not only in terms of accuracy (Baich et al., 2022; Al Farsi et al., 2024). It is worth noting that false positive rate is important since too many alerts may burden security staff and affect the effectiveness of the system (Saran & Kesswani, 2023).

SVM has reached 96.4% accuracy, 2.8% of the false positive rate and required 67 ms of processing time. Despite the lower performance compared to Random Forest and CNN, the relatively moderate consumption of computing resources means that SVM will still remain relevant in the cases when resources and needs match each other. The lowest performance in terms of accuracy (94.1%), the highest false positive rate (4.5%) and the requirement of 89 ms of processing time have been demonstrated by KNN (Mondal & Singh, 2022).

Moreover, this finding further proves the importance of feature selection. By reducing the

dimensionality of features by 35%, there is an increase in the processing time of 28%, but with no decrease in the accuracy rate. Thus, removal of unnecessary network features may increase the computational efficiency while retaining the detection performance. This finding confirms the findings of the comparative analysis, proving the importance of efficient feature representation in ML-based IDS (Al Lail et al., 2023; Santhosh Kumar et al., 2023).

This means that using the different learning capabilities may help intrusion detection system to recognize attacks of a previously unknown pattern. This result is very valuable since modern cyberattacks continue evolving and may not fit previously learned patterns.

Thus, it can be stated that accuracy-latency trade-off was found in this study. CNN shows the maximum accuracy, while Random Forest shows the best combination of accuracy, low false positive rate, and fast processing. Thus, for enterprise implementation where both characteristics are required, Random Forest is the best model of those tested (Jmila & Khedher, 2022).

6. Conclusion

This comparative study considered Random Forest, SVM, KNN, and CNN machine learning algorithms for detecting network intrusions based on the CICIDS2017 dataset. This analysis shows that CNN demonstrated the highest accuracy equal to 99.2%, whereas Random Forest showed 98.7% accuracy, the lowest false positive rate equal to 1.2% and the shortest processing time of 42 ms per instance.

The results show that accuracy is not enough to choose the best model for an intrusion detection system. However, in spite of the little increment in accuracy, the processing time required by CNN is approximately 2.7 times higher compared to the one of Random Forest algorithm, hence, making the second one more effective. Therefore, the most efficient method regarding the trade-off between accuracy, false positive rate, and processing time is Random Forest.

Dimensionality reduction by 35% and increase in speed by 28% due to feature selection.

Furthermore, ensemble approaches helped to improve detection of the zero-day attacks by 22%. Random Forest provides the most beneficial cost-performance ratio, but CNN can be considered if maximum accuracy is the main priority instead of latency.

7. Recommendations

1. Random Forest would make a good choice for enterprise IDS implementation due to its high accuracy and low false positive rate along with quick processing.
2. CNN could be considered where detection accuracy is the most important feature, especially where enough computational power is at hand.
3. Feature selection should be applied to intrusion detection systems because the study showed that 35% of dimensions were reduced and there was 28% faster processing.
4. Ensemble learning should be utilized for advanced threat detection, especially for better zero-day attacks detection.
5. The future researches should check the models in real-time network traffic to see whether the results are maintainable in such conditions.
6. The future researches should check the models on different data sets to minimize the effect of the particular data set features on the model's performance.
7. Future studies should perform adversarial attacks testing on machine learning based IDS because an adversary can manipulate the traffic pattern for avoiding detection.
8. Future implementations should consider not only accuracy and processing time but hardware and resource requirements too for selecting the best model.

REFERENCES

Ali, M. L., Thakur, K., Schmeelk, S., DeBello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences*, 15(4), 1903.

- Hidayat, I., Ali, M. Z., & Arshad, A. (2023). Machine learning-based intrusion detection system: an experimental comparison. *Journal of Computational and Cognitive Engineering*, 2(2), 88-97.
- Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *Ieee Access*, 11, 80348-80391.
- Singh, A., Prakash, J., Kumar, G., Jain, P. K., & Ambati, L. S. (2024). Intrusion detection system: A comparative study of machine learning-based IDS. *Journal of Database Management (JDM)*, 35(1), 1-25.
- Samantaray, M., Barik, R. C., & Biswal, A. K. (2024). A comparative assessment of machine learning algorithms in the IoT-based network intrusion detection systems. *Decision Analytics Journal*, 11, 100478.
- Note, J., & Ali, M. (2022). Comparative analysis of intrusion detection system using machine learning and deep learning algorithms. *Annals of Emerging Technologies in Computing (AETiC)*, 6(3), 19-36.
- Siddharth, K., Gagan Kumar, P., Chandrababu, K., Janardhana Rao, S., & Sanjay Ramdas, B. (2023). A comparative analysis of network intrusion detection using different machine learning techniques. *J Contemp Edu Theo Artific Intel: JCETAI-102*.
- Udurume, M., Shakhov, V., & Koo, I. (2024). Comparative analysis of deep convolutional neural network–bidirectional long short-term memory and machine learning methods in intrusion detection systems. *Applied Sciences*, 14(16), 6967.
- Makhdoomi, P. M. S., Ikhlas, M., Khursheed, A., Hilal, F., Ahmad Najar, Z., Hameed, J., & Sharma, S. (2026). Network-based intrusion detection: a comparative analysis of machine learning approaches for improved security. *Journal of Cyber Security Technology*, 10(1), 1-28.

- Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A comparative study of using deep learning algorithms in network intrusion detection. *IEEE access*, 12, 58851-58870.
- Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A comparative study of using deep learning algorithms in network intrusion detection. *IEEE access*, 12, 58851-58870.
- Baich, M., Hamim, T., Sael, N., & Chemlal, Y. (2022). Machine Learning for IoT based networks intrusion detection: a comparative study. *Procedia Computer Science*, 215, 742-751.
- Al Farsi, A., Khan, A., Bait-Suwailam, M. M., & Mughal, M. R. (2024). Comparative Performance Evaluation of Machine Learning Algorithms for Cyber Intrusion Detection.
- Al Lail, M., Garcia, A., & Olivo, S. (2023). Machine learning for network intrusion detection—a comparative study. *Future Internet*, 15(7), 243.
- Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. *Computational intelligence and neuroscience*, 2023(1), 8981988.
- Saran, N., & Kesswani, N. (2023). A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things. *Procedia Computer Science*, 218, 2049-2057.
- Mondal, B., & Singh, S. K. (2022). A comparative analysis of network intrusion detection system for iot using machine learning. In *Internet of Things and Its Applications: Select Proceedings of ICIA 2020* (pp. 211-221). Singapore: Springer Nature Singapore.
- Jmila, H., & Khedher, M. I. (2022). Adversarial machine learning for network intrusion detection: A comparative study. *Computer Networks*, 214, 109073.
- Banerjee, S., & Parisa, S. K. (2023). Ai-enhanced intrusion detection systems for retail cloud networks: A comparative analysis. *Transactions on Recent Developments in Artificial Intelligence and Machine Learning*, 15, 15.
- Alharthi, A., Alaryani, M., & Kaddoura, S. (2025). A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. *Array*, 26, 100406.