JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 02
2025

Research Article
https://doi.org/10.56979/802/20245

An Ensemble Approach for Firewall Log Classification using Stacked Machine Learning Models

Mudasir Ali[1], Muhammad Faheem Mushtaq[2*], Urooj Akram[2], Shabana Ramzan[3], Saba Tahir[2], and Muhammad Ahsan[2]

[1]Department of Computer Science, The Islamia University of Bahawalpur, 63100, Bahawalpur, Pakistan.
[2]Department of Artificial Intelligence, The Islamia University of Bahawalpur, 63100, Bahawalpur, Pakistan.
[3]Department of Computer Science & IT, Government Sadiq College Women University, Bahawalpur, Pakistan.
[*]Corresponding Author: Muhammad Faheem Mushtaq. Email: faheem.mushtaq@iub.edu.pk

Received: January 03, 2025 **Accepted:** March 01, 2025

Abstract: Firewall logs are still challenging to evaluate, while being important data sources. Machine Learning has become a popular technology for creating strong security measures because of their ability to react quickly to complicated attacks. Firewall logs generate high-volume, complex, and often imbalanced data, where malicious activities are rare compared to normal traffic. The challenge is further compounded by the dynamic nature of cyber threats and the presence of noise or redundant information in the logs. In this research, a stacking classifier called Decision Tree Classifier + Bagging Classifier (DB) for Firewall logs is proposed using the ensemble machine learning models. A comparison is performed to evaluate the classifier's overall performance based on F1-score, accuracy, precision, and recall. A firewall that was set up with Snort and TWIDS had its logs taken. The 65532 occurrences of the receiving log record include a total of 12 attributes. Creating multi-class machine learning models that can analyze the firewall logs dataset and classify the necessary actions in response to learned classes as "Reset-both," "Allow," "Deny," or "Drop". For assessment, a variety of machine learning methods have been used, such as Random Forest, K-Nearest Neighbor, Logistic Regression, and AdaBoost Classifier. The experiment's 99.89% accuracy rate for the proposed model using stacking classifier DB is an interesting interpretation of the findings. However, the high accuracy rates produced as compared to other algorithms show that the recommended points were crucial in increasing the firewall classification rate.

Keywords: Firewall Logs; Decision Tree; Bagging Classifier; Machine Learning; Ensemble Learning.

1. Introduction

The social community is constantly changing in the era of computer networks and information technology, bringing concerns about network and information security. Among other things, network administrators invest a lot of money in network security measures like firewalls and antivirus software[1]. They put a lot of work into protecting the networks' integrity and safety as well as keeping network data private to thwart intrusions from both within and outside the network. Network security has become a global problem as everyday actions are now completed online thanks to the development of internet technology. Therefore, the goal is to identify security vulnerabilities so that common security technologies like firewalls and VPNs may be used to protect against assaults [2]. The most important component of computer networks that naturally contributes to network security is the firewall. By examining the incoming and outgoing packets, it may either prevent or permit communication based on a predetermined process. For computer networks and communication to function safely and effectively, a firewall structure is required. A hardware or software network security tool called a firewall is responsible for monitoring packet traffic entering and leaving the network and determining whether or not unique traffic will be allowed [3]. The firewall records network plan hostilities, including source, port numbers, IP addresses for vacation spots, and other data. Based on source and destination IP addresses, protocols, ports, and other

factors, the logs explain how the firewall controls incoming and outgoing network connections [4]. Most researchers look at firewall logs for too-lenient or pointless rules to ignore that enhances the detection of potentially harmful behavior [5]. The threat posed by cyberattacks has grown in this important business. Over the past 10 years, cyber threats to businesses in all sectors have significantly increased. Cyber threats such as ransomware, data leaks, hacking, phishing, and insider risk put groups in danger [6]. This demonstrates the need to adhere to data integrity and usability precautions. In most cyberattacks, the attacker may conceal his attack since he is aware of the company's security procedures [7]. The regulations are always changing, which is a big problem because they are manually defined by the engineers and safety personnel of the firms in line with their policies and demands. Furthermore, firewalls act as manipulation gates that allows the authorized network communications to flow through [8].

Growing awareness of AI's potential benefits in the field of cyber security stems from the possibility that it might improve network and security protocols, making structures more resilient, responsive, and robust. Furthermore, massive volumes of log data are produced by network security solutions like Intrusion Detection Systems (IDS) and firewalls. This information may be gathered and utilized to build models that help identify community dangers, along with patterns in the characteristics of network site visitors [9]. Machine learning algorithms need a lot of historical data, which can lead to problems like model induction brought on by thousands of variables [10]. In addition to the RF's efficient handling of non-linear connections, as is the case with this dataset, it also contains a large number of selection trees. The Deep Neural Network (DNN) is used to determine its impact on multiple features-single training in the numerical information sets [11]. This included dealing with anomalies and variance in values, as well as removing components that no longer added value to the classification method or resulted in processing time waste aside from benefit [12]. Furthermore, datasets are frequently analyzed using machine learning techniques to uncover hidden associations. Under the direction of algorithms, machine learning constantly optimizes models and generates plausible predictions from vast volumes of data. A comparative performance analysis was conducted on several machine learning and deep learning algorithms, such as K-Nearest Neighbor (KNN), Naive Bayes (NB), J48, Random Forest (RF), and Artificial Neural Network (ANN) [13].

In this research to categorized the proposed action as “Allow”,” Drop”, “Deny”, or “Reset-both using machine learning classification techniques [14]. Using a dataset taken from a private organizations network log, each of us compared the performance of several machine learning algorithms, including Random Forest, K-Nearest Neighbor, Logistic Regression, AdaBoost Classifier and the proposed approach, Decision Tree + Bagging classifier. In this regard, this research provides a stacking model and essentially makes the following contributions:

- In order to improve security protocols for Internet of Things devices, this research proposed a stacking architecture for database intrusion attack detection by incorporating the advantages of Random Forest, K-Nearest Neighbor, Logistic Regression, and AdaBoost Classifier.
- Developed a multi-class machine learning model to categorize firewall log actions into "Reset-both," "Allow," "Deny," or "Drop." Addressed challenges in processing firewall logs, including high-volume, complex, imbalanced data and the dynamic nature of cyber threats.
- The efficiency of the proposed approach is carefully evaluated using a number of widely used assessment metrics, including accuracy, precision, recall, and F1 score.

This study is separated into several subsequent sections: Section II discusses the related work that are relevant to the proposed studies. Section III entails providing an overview of the study strategy, including the data gathering strategies, data analysis approaches, and proposed approach for Firewall Log Classification. Results and discussion of the proposed approach are presented in Section IV. Section V conclude the conclusion and future research directions.

2. Related Work

The use of ML and DL approaches to analyze firewall logs and categorize the necessary actions based on the classes that are acquired as "Allow," "Drop," "Deny," or "Reset-both" are demonstrated [15]. Empirical evaluations were carried out, using a number of ML and DL methods for comparison including KNN, NB, J48, RF, and ANN to evaluate the performance of the developed models. In the first and second trials, the RF algorithm yielded the greatest accuracy of 99.11% and 99.64%, respectively, suggesting that

the proposed method greatly increased the firewall classification rate [16]. This study discovered that the linear activation function produced the best accuracy value of 67.5% and the sigmoid activation function had the highest recall value of 98.5%. At 76.4%, the RBF activation function had the highest F1 score [17].

The analysis's goal was to determine which classifier would best predict the action label of the firewall log entries. The results showed that Random Forest was the most accurate classifier with a predicted accuracy 99.7% [18]. Optimizing Decision Tree (ODT) and shallow neural networks (SNN) are two machine learning approaches that the author presents in their adaptive classification model for classifying packets in firewall system [19]. The experimental results show that the proposed model outer performs several of the existing firewall classification techniques in terms of overall accuracy, obtaining 99.8% and 98.5% accuracy for ODT and SNN, respectively [20].

Regarding the second level, the Anomaly type was determined and specified using the Hidden Markov Model (HMM) on firewall system [21]. The performance of the Anomaly Detection System (ADS) was evaluated against three single-level anomaly detection techniques based on machine learning (ML) algorithm: Logistic regression, decision tree and support vector machine in order to examine the ADS system outer performed these single-level ML algorithm, with an FPR of 4.09% and a classification accuracy of 93.5% [22]. Following analyzing a freeware program for endpoint security, the four characteristics that were collected added to ML classifiers such as KNN, NB, and J48 [23]. The class attribute was the action attribute that accepts values of "Allow" or "Drop". The accuracy of the four algorithms, performances were compared and assessed. It was found that the KNN classifier had the best accuracy, at 99.87% [24].

In order to determine that concerns may be discovered by statistical analysis of the logs, this study aimed to observe the firewall using machine learning techniques and the JRIP algorithm. In addition, four characteristics were derived from the extraction of nine features [25]. These trials yielded finding with a 99.92% accuracy rate. Better outcomes, may come from additional feature extraction research and analysis [26]. A larger feature vector might be produced, for instance, by combining features from the applied ADS with additional data from the firewall log, as the study mentions. They proposed using modified mortality chain model as a compromise indication in order to accomplish this. They created one-class SVM models and multi-class SVM models with respective accuracy rates of 95.33% and 98.67% [27].

In another research, classify the firewall log using SVM technique was utilized. At each instance, a new SVM activation function was used to assess the model's performances [28]. The action property, which accepts the values "allow", "drop", "deny', or "rest-both" was multiclass classified by them. Using the sigmoid activation algorithm produced the maximum recall value of 98.5% [29]. Using the linear activation function produced the highest accuracy of 67.5%. Additionally, using the Radial Basis Function (RBF) activation function produced the greatest F-measure of 76.4%. The purpose of the research, the models employed, and the highest performance attained are all compiled in Table 1, which also includes all of the prior work that have been addressed.

Table 1. Summary of the Related Work

References	Models	Number of Features	Results
[30]	SVM, LR, OR DT	6 features	Accuracy= 93.54%
[31]	NB, KNN, One R AND J48	6 features	Accuracy= 99.87%
[32]	SVM	6 features	Accuracy= 95.33%
[33]	SVM	11 features	Recall = 98.5% Precision = 67.5%
[34]	DT	11 features	Accuracy= 99.83%
[35]	Ensemble RF	11 features	Accuracy= 99.80%
[36]	Cart	34 features	Accuracy= 96%
[37]	Decision Tree	11 features	Accuracy= 90.80%
[38]	Naïve Bayes	11 features	Accuracy= 87.81%

3. Proposed Methodology

The main aim of this research is used to Machine Learning techniques to internet firewall analysis on the firewall log dataset. The utilized models include Random Forest, K-Nearest Neighbors, Logistic Regression, and AdaBoost Classifier. An ensemble model that combines Decision Tree and Bagging Classifier was presented in order to improve predictive performance. As data moves over the network, the models seek to predict the best path of action for each session. By using the effectiveness of bagging, the decision tree stability is increased. To ensure an appropriate basis for assessment, the dataset was divided into 80% for training and 20% for testing. Four primary measures were used to evaluate this classifier performance in order to fully analyze the way algorithm handled firewall-related classification tasks: accuracy, precision, recall and F1score. The experimental findings demonstrate how the proposed ensemble model may outer perform individual's classifiers in term of performance and reliability. Each step of the conducted approach is summarized in Figure 1.

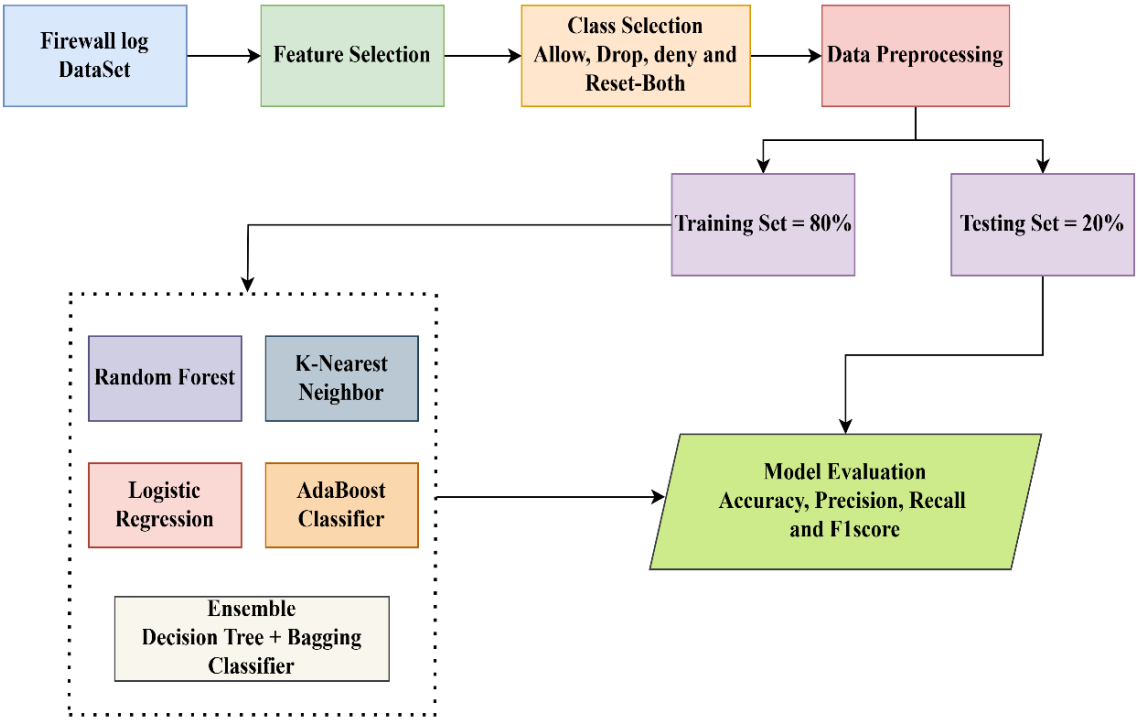

Figure 1. Proposed Methodology

3.1. Dataset Description

The present research made use of a network log dataset that was collected by an individual organization. Log records were stolen from a firewall that was installed using Snort and TWIDS. There are 12 characteristics altogether in the 65532 instances of the receiving log record. Allow action, drop, and reset are the four classes in total. The dataset records' statistics are displayed in the Table 1.

Table 2. Statistics of Dataset Records

Feature	Action	
Value	Allow	37640
	Drop	14987
	Deny	12851
	Reset-Both	54

3.2. Data Preprocessing

To prepare the dataset for use by models for training and testing, pre-processing is obviously done before any analysis. Preprocessing includes importing the dataset cleaning it, modifying it, and transforming it into a format appropriate for the intended. Dataset splitting it into for training 80% and testing 20%. Numerical values were then obtained from categorical characteristics using label encoding. Only 22.86% of the log dataset with over 1,000 items contain instances in which "Deny" was the action

done. Since at least one category that was previously balanced is now excessively in an array compared to others, this proposed an imbalance the number of occurrences of each action type, the 37500 example were selected at random to produce a total 65532 instances. Figure 2 represent the dataset with record.

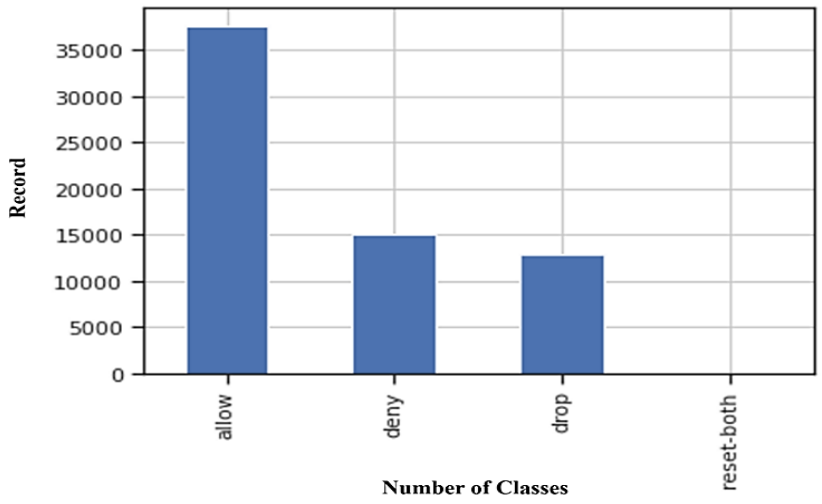

Figure 2. Detail of Dataset

3.3. Feature Selection and Classification

The characteristics of source and destination IP addresses, source and destination ports, and protocol (TCP or UDP) are taken into consideration in each log line. Only six crucial factors action (Allow, Deny), Source IP, Source port, Destination IP, Destination port, and Protocol (TCP/UDP) have been chosen to categorize the firewall log collection. As the category attribute, the motion attribute with the nominal attributes "Allow" and "Drop" has been selected. The dataset included 25 numerical and express points that described the aim characteristic, the activity, and the network visitors' sessions. To achieve the best possible performance, two unique experiments have been conducted.

3.4. Classification of Machine Learning Models

In classification, finally the feature extraction is analyzed the dataset from the network traffic log and feeding it into classifiers such as Random Forest, K-Nearest Neighbor, Logistic Regression, and AdaBoost Classifier. The ML algorithms employed are evaluated the overall performance in terms of accuracy, precision, recall, F-measure

3.4.1. Random Forest

A well-known machine learning method called Random Forest (RF) used in network firewalls to categorize network traffic site visitors as either harmful or safe [39]. It is entirely predicated on the idea of ensemble learning, which is the process of merging several classifiers to solve a complex issue and improve the model's overall performance. The basic concept is to train an ensemble of decision trees using the RF method, with each tree being trained on a random subset of features and a part of the dataset.

3.4.2. K-Nearest Neighbor

One type of supervised learning method used in machine learning for classifying statistical points is the K-Nearest Neighbor (KNN) algorithm. It assigns the new case to the class that is most similar to the handy categories based on the assumption that the new data and handy instances are similar. KNN can no longer make any assumptions about the underlying data because it is a non-parametric approach [40]. When it receives new information, it stores it in a class that is similar to the previously acquired data. For web firewall applications, the KNN algorithm provides an easy and efficient way for classifying network surfing as either begin or malicious.

3.4.3. Logistic Regression

Logistic regression is a well-liked supervised learning technique in machine learning for data point classification. Based on the correlation between the attributes and the target variable, it forecasts the likelihood that a data point will fall into a specific category [41]. By fitting a logistic function to the data, logistic regression is a statistical technique that may be used to estimate the likelihood of outcomes. It is beneficial for categorizing tasks, although it can also be used in multi-class situations. Web firewall

applications benefit greatly from the widespread use of logistic regression in a variety of domains, including the classification of network traffic as either benign or malicious.

3.4.4. Adaptive Boosting

The Adaptive Boosting (AdaBoost) algorithm is one kind of supervised learning technique that is frequently employed in machine learning for data point classification. It iteratively modifies the weights of misclassified examples to create a strong classifier by combining several weak classifiers. AdaBoost is a flexible and successful method for a range of classification tasks as it is not presuming anything about the distribution of the underlying data. After processing the dataset, it uses the cumulative judgment of the weak classifiers to assign fresh data to a class [42]. In web firewall applications, this technique is very helpful for spotting trends and irregularities, including determining if network traffic is malicious or benign.

3.5. Proposed Ensemble Approach

Several machine learning classifiers, such as Random Forest (RF), K-Nearest Neighbor (KNN), Logistic Regression (LR), and AdaBoost Classifier, are implemented and evaluated as part of the proposed approach for the firewall log system in order to efficiently categorize and analyze firewall logs. An ensemble model that combines Decision Tree + Bagging Classifier with a meta-classifier like Logistic Regression is proposed in order to improve prediction performance and solve the drawbacks of individuals models. This ensemble improves the accuracy and generalization of the decision tree while lowering overfitting by utilizing the stability and robustness of bagging. The method seeks to enhance the system capacity to precisely identify and categorize network activity by incorporating these classifiers into the firewall log system, ensuring increased security and efficiency.

4. Results and Discussion

Several models have been built using machine learning methods to run the experiment. In this research, 65532 different scenarios were utilized to conduct the studies, and four different target types such as “Allow”, “Drop”, “Deny”, and “Reset-Both” were utilized. A special combination of components has been employed for this experiment. Source port, destination port, NAT source port, NAT destination port, action, bytes, bytes sent, bytes received, packets, elapsed time, pkts_sent, and pkts_received are the 12 elements that were employed in this experiment. Training on various training sizes from the dataset used for the analysis of the overall performance of the machine learning models. Random look-at set sizes from the dataset are used to assess the model's predictability. In this search, the multiclass machine learning styles were assessed in term of precision, recall, accuracy and f1score.

4.1. Performance Evaluation of Random Forest

Random Forest (RF) is the well-known machine learning approach for classification and regression problems. RF are known for their ability to avoid overfitting and capable of handling complex information and high-dimensional feature spaces. RF obtained an accurate prediction rate of accuracy (0.9984), precision (0.9407), recall (0.9269), and f1-score (0.9567) in its predictions of the model performance on the testing set. Figure 3 shows the random forest performed better in response prediction characteristics.

4.2. Performance *Evaluation of K-Nearest Neighbor*

K-Nearest Neighbor (KNN) models are recognized for their simplicity and effectiveness, particularly when working with smaller datasets. They are capable of handling both classification and regression tasks by leveraging proximity-based decision-making. KNN achieved an overall rate of accuracy (0.9984), precision (0.8397), recall (0.8487), and f1-score (0.8321) in predicting the model performance outcomes on the testing set. As illustrated in Figure 4, the K-Nearest Neighbor model demonstrated superior performance in predicting response characteristics.

4.3. Performance Evaluation of Logistic Regression

Logistic Regression is a well-known machine learning approach for classification and regression problems. It is recognized for its simplicity and effectiveness in handling linearly separable data. LR generated an achievement rate of accuracy (0.9778), precision (0.7279), recall (0.7267), and f1score (0.7303) in predicting the model performance outcomes on the testing set. As shown in Figure 5, the logistic regression model demonstrated superior performance in response prediction characteristics.

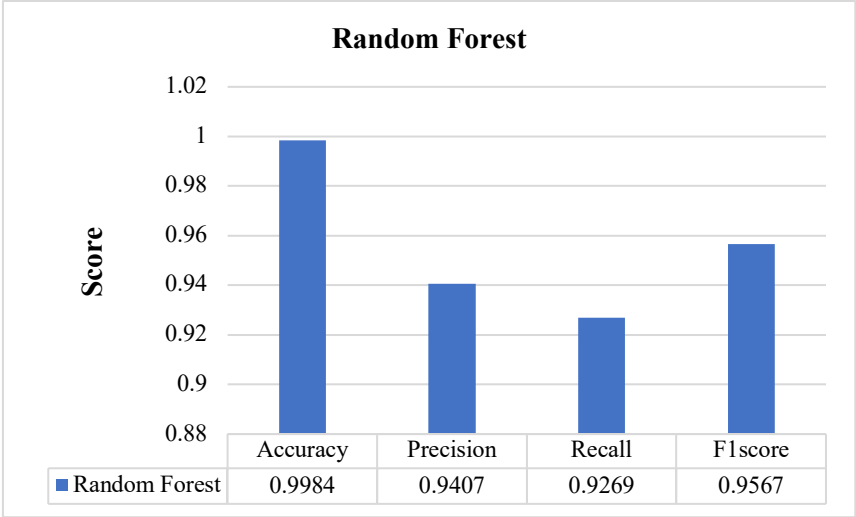

Figure 3. Performance Evaluation of RF Model.

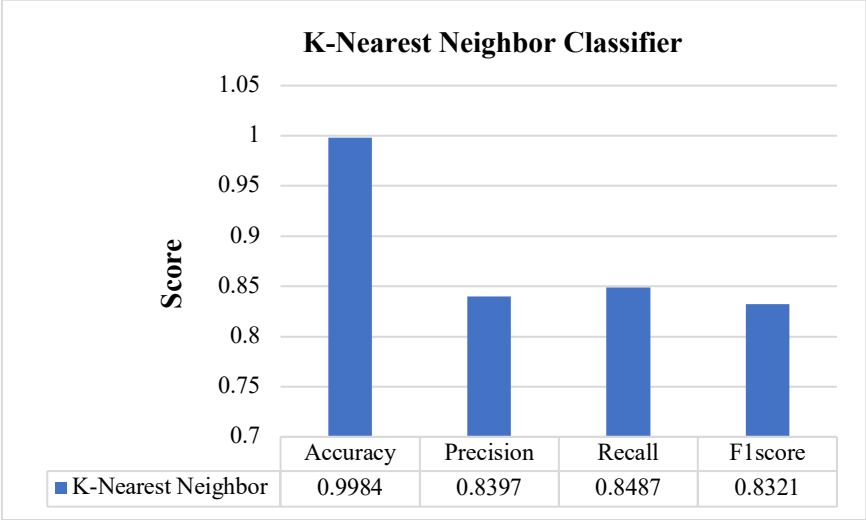

Figure 4. Performance Evaluation of KNN.

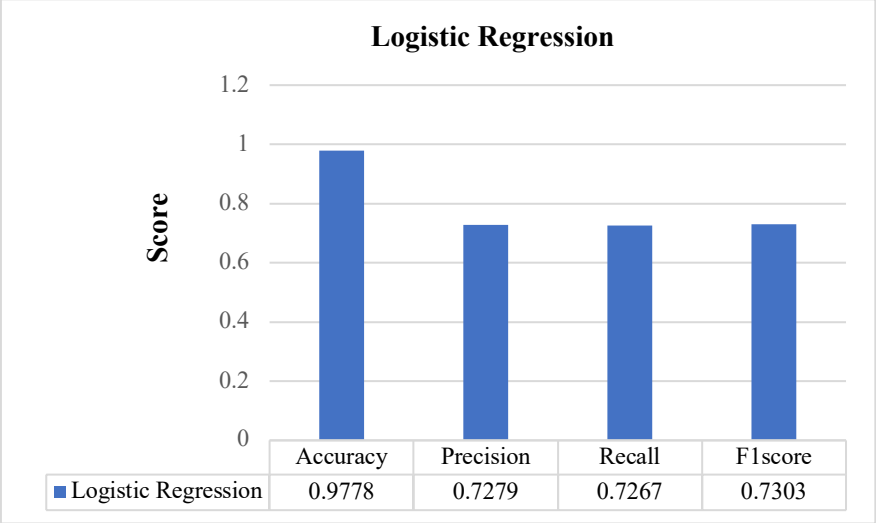

Figure 5. Performance Evaluation of LR Model.

4.4. Performance Evaluation of AdaBoost Classifier

A well-known machine learning approach for classification and regression problems is the AdaBoost Classifier. AdaBoost scored an overall score of accuracy (0.9984), precision (0.8397), recall (0.8487), and f1-

score (0.8321) in its predictions of the model performance on the testing set. As shown in Figure 6, the AdaBoost Classifier demonstrated superior performance in response prediction characteristics.

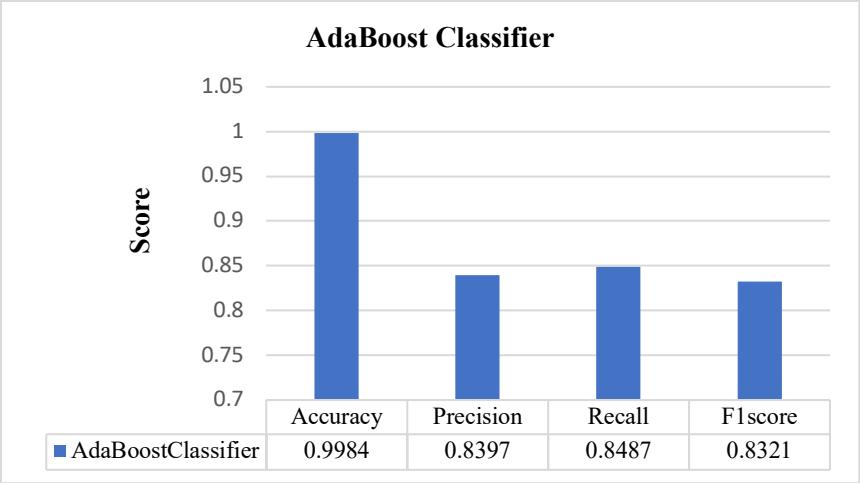

Figure 6. Performance Evaluation of AdaBoost Classifier.

4.5. Performance Evaluation of Ensemble Models

A widely recognized machine learning approach for classification and regression tasks is the proposed ensemble decision tree + bagging classifier. This method is celebrated for its robustness against overfitting, its ability to manage complex data structures, and its effectiveness in high-dimensional feature spaces. The proposed ensemble model achieved a satisfactory level of accuracy (0.9989), precision (0.9488), recall (0.9157), and f1-score (0.9307) in predicting the model performance outcomes on the testing set. As illustrated in Figure 7, the proposed ensemble decision tree + bagging classifier demonstrated superior performance in response prediction metrics.

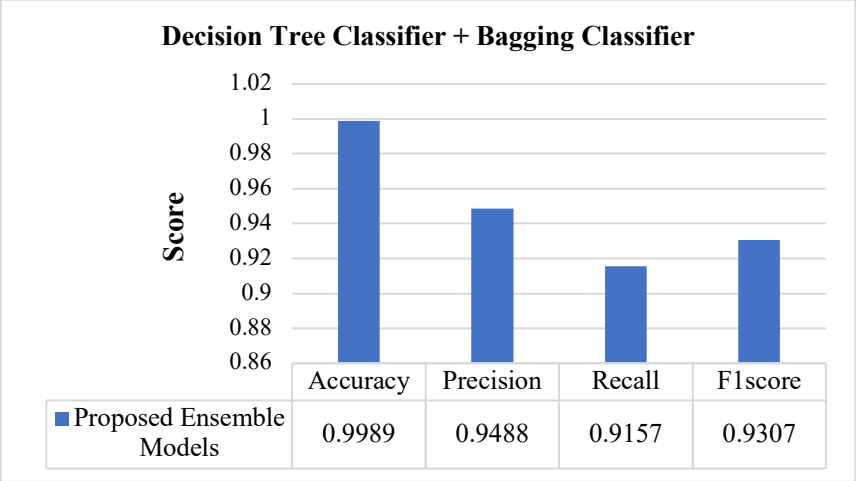

Figure 7. Performance Evaluation of Proposed Ensemble Models.

4.6. Comparison Analysis of All Models

The results of the multi-classifier model were efficient and effective in terms of result, based on the evaluation of five machine learning classification algorithms. A comparison is made between the most widely used machine learning categorization models in the literature. The proposed ensemble Decision Tree + Bagging Classifier (DB) model performs better as compare to other models in term of accuracy, precision, recall, and F1-score as shown in Table 2. In contrast to the proposed model, other machine learning models such as RF, KNN, LR, and AdaBoost Classifier perform less effectively.

Table 3. Comparison Analysis of All Models

Models	Accuracy	Precision	Recall	F1-score
Random Forest	0.9984	0.9407	0.9269	0.9567

K-Nearest Neighbor	0.9935	0.7449	0.7441	0.7458
Logistic Regression	0.9778	0.7279	0.7267	0.7303
AdaBoost Classifier	0.9984	0.8397	0.8487	0.8321
Proposed Ensemble (DB) Model	0.9989	0.9488	0.9157	0.9307

5. Conclusions

Firewalls are a crucial component of corporate network security, being the first line of defense in the network. Additionally, firewalls are capable of defending against both internal and external threats. Given the significance of firewalls for system security, this study concentrated on developing various machine learning models that can categorize the necessary reaction to sessions in firewall logs. The primary features are Action (Drop, Allow, Deny, Reset Both), Source Port, Destination Port, and Nat Source Port. As a type attribute, the motion attribute containing "Drop," "Allow," "Reset Both," and "Drop" has been selected. Using classifiers such as Random Forest, K-Nearest Neighbor, Logistic Regression, and AdaBoost Classifier in parallel processing, according to the investigate findings, proposed models and libraries are more accurate than the methods currently in use. Due to the assessment findings, the proposed models and libraries are more accurate than the methods currently in used. The experiment's 99.89% accuracy rate for the proposed model using stacking classifier Decision Tree + Bagging Classifier (DB) with meta classifier Logistic Regression provides an interesting interpretation of the findings. DB for Firewall logs, a stacking classifier, outperformed the other classification methods proposed in the model in terms of total performance. However, the higher accuracy rates obtained when compared to alternative methods demonstrate how important the proposed points were in raising the firewall categorization. This research can be enhanced in future by incorporating transfer learning and reinforcement learning which may be more successful should be conducted.

References

1. M. S. Islam, M. A. Uddin, D. M. D. Hossain, D. M. S. Ahmed, and D. M. G. Moazzam, "Analysis and evaluation of network and application security based on next generation firewall," International Journal of Computing and Digital Systems, vol. 13, no. 1, pp. 193-202, 2023.
2. A. Goel, A. Kashyap, B. D. Reddy, R. Kaushik, S. Nagasundari, and P. B. Honnavali, "Detection of VPN Network Traffic," in 2022 IEEE Delhi Section Conference (DELCON), 2022: IEEE, pp. 1-9.
3. M. Xiao, M. Guo, and H. Lv, "The Principle of Firewall Technology and Its Application in Computer Network Security," in 2021 3rd International Conference on Applied Machine Learning (ICAML), 2021: IEEE, pp. 174-177.
4. U. Akram et al., "IoTTPS: Ensemble RKSVM model-based Internet of Things threat protection system," Sensors, vol. 23, no. 14, p. 6379, 2023.
5. A. K. Meena, N. Hubballi, Y. Singh, V. Bhatia, and K. Franke, "Network Security Systems Log Analysis for Trends and Insights: A Case Study," in 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2020: IEEE, pp. 1-6.
6. M. F. Mushtaq, U. Akram, I. Khan, S. N. Khan, A. Shahzad, and A. Ullah, "Cloud computing environment and security challenges: A review," International Journal of Advanced Computer Science and Applications, vol. 8, no. 10, 2017.
7. M. Aljabri, A. A. Alahmadi, R. M. A. Mohammad, M. Aboulnour, D. M. Alomari, and S. H. Almotiri, "Classification of firewall log data using multiclass machine learning models," Electronics, vol. 11, no. 12, p. 1851, 2022.
8. E. Ucar and E. Ozhan, "The analysis of firewall policy through machine learning and data mining," Wireless Personal Communications, vol. 96, pp. 2891-2909, 2017.
9. A. Taner, Y. B. Öztekin, and H. Duran, "Performance analysis of deep learning CNN models for variety classification in hazelnut," Sustainability, vol. 13, no. 12, p. 6527, 2021.
10. M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran, and I. Ashraf, "Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment," IEEE Access, 2024.
11. M. Shahroz et al., "Hierarchical Attention Module-Based Hotspot Detection in Wafer Fabrication Using Convolutional Neural Network Model," IEEE Access, 2024.
12. J. Wei et al., "Machine learning in materials science," InfoMat, vol. 1, no. 3, pp. 338-358, 2019.
13. S. Ahmadi, "Next Generation AI-Based Firewalls: A Comparative Study," International Journal of Computer (IJC), vol. 49, no. 1, pp. 245-262, 2023.
14. J. Liu, "Enhancing Network Security Through Router-Based Firewalls: An Investigation into Design, Effectiveness, and Human Factors," Highlights in Science, Engineering and Technology, vol. 85, pp. 724-732, 2024.
15. M. H. Rahman, T. Islam, M. M. Rana, R. Tasnim, T. R. Mona, and M. M. Sakib, "Machine Learning Approach on Multiclass Classification of Internet Firewall Log Files," in 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), 2023: IEEE, pp. 358-364.
16. K. Neupane, R. Haddad, and L. Chen, "Next generation firewall for network security: a survey," in SoutheastCon 2018, 2018: IEEE, pp. 1-6.
17. U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review," Sensors, vol. 23, no. 8, p. 4117, 2023.
18. S. Tiwari, N. Kumar, K. Joshi, and S. Kumar, "Enhancing Cyber Security: A Comparative Study of Artificial Neural Networks (ANN) and Machine Learning for Improved Network Vulnerability Detection," in Advanced Technologies for Realizing Sustainable Development Goals: 5G, AI, Big Data, Blockchain, and Industry 4.0 Application: Bentham Science Publishers, 2024, pp. 126-146.
19. A. Sarwar et al., "IoT networks attacks detection using multi-novel features and extra tree random-voting ensemble classifier (ER-VEC)," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 12, pp. 16637-16651, 2023.
20. S. Allagi and R. Rachh, "Analysis of Network log data using Machine Learning," in 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 2019: IEEE, pp. 1-3.
21. A.-D. Tudosi, A. Graur, D. G. Balan, A. D. Potorac, and R. Tarabuta, "Distributed Firewall Traffic Filtering and Intrusion Detection Using Snort on pfSense Firewalls with Random Forest Classification," in 2023 46th International Conference on Telecommunications and Signal Processing (TSP), 2023: IEEE, pp. 101-104.
22. J. M. Kizza, "Firewalls," in Guide to Computer Network Security: Springer, 2024, pp. 265-294.

23. M. A. Shahid, U. Akram, M. M. A. Shahid, A. Samad, M. F. Mushtaq, and R. Majeed, "A Systematic Approach Towards Compromising Remote Site HTTPS Traffic Using Open Source Tools," in 2020 IEEE 23rd International Multitopic Conference (INMIC), 2020: IEEE, pp. 1-6.
24. L. Golightly, P. Modesti, and V. Chang, "Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator," Journal of Cybersecurity and Privacy, vol. 3, no. 3, pp. 464-492, 2023.
25. R. Majeed, N. A. Abdullah, and M. F. Mushtaq, "IoT-based cyber-security of drones using the Naïve Bayes algorithm," International Journal of Advanced Computer Science and Applications, vol. 12, no. 7, 2021.
26. M. Ali et al., "Pneumonia Detection Using Chest Radiographs With Novel EfficientNetV2L Model," IEEE Access, 2024.
27. R. A. Naqvi et al., "Coronavirus: A mild virus turned deadly infection," Computers, Materials and Continua, vol. 67, no. 2, pp. 2631-2646, 2021.
28. M. A. Abid, S. Ullah, M. A. Siddique, M. F. Mushtaq, W. Aljedaani, and F. Rustam, "Spam SMS filtering based on text features and supervised machine learning techniques," Multimedia Tools and Applications, vol. 81, no. 28, pp. 39853-39871, 2022.
29. İ. F. Kılınçer, F. Ertam, and A. Şengür, "Automated fake access point attack detection and prevention system with IoT devices," Balkan Journal of Electrical and Computer Engineering, vol. 8, no. 1, pp. 50-56, 2020.
30. Q. Cao, Y. Qiao, and Z. Lyu, "Machine learning to detect anomalies in web log analysis," in 2017 3rd IEEE international conference on computer and communications (ICCC), 2017: IEEE, pp. 519-523.
31. H. E. As-Suhbani and S. Khamitkar, "Classification of firewall logs using supervised machine learning algorithms," International Journal of Computer Sciences and Engineering, vol. 7, no. 8, pp. 301-304, 2019.
32. T. Schindler, "Anomaly detection in log data using graph databases and machine learning to defend advanced persistent threats," arXiv preprint arXiv:1802.00259, 2018.
33. F. Ertam and M. Kaya, "Classification of firewall log files with multiclass support vector machine," in 2018 6th International symposium on digital forensic and security (ISDFS), 2018: IEEE, pp. 1-4.
34. H. N. K. AL-Behadili, "Decision tree for multiclass classification of firewall access," International Journal of Intelligent Engineering and Systems, vol. 14, no. 3, pp. 294-302, 2021.
35. D. Sharma, V. Wason, and P. Johri, "Optimized classification of firewall log data using heterogeneous ensemble techniques," in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021: IEEE, pp. 368-372.
36. C. Marques, S. Malta, and J. Magalhães, "DNS firewall based on machine learning," Future Internet, vol. 13, no. 12, p. 309, 2021.
37. Q. A. Al-Haijaa and A. Ishtaiwia, "Machine learning based model to identify firewall decisions to improve cyber-defense," International Journal on Advanced Science, Engineering and Information Technology, vol. 11, no. 4, pp. 1688-1695, 2021.
38. S. Prabakaran et al., "Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network," Sensors, vol. 22, no. 3, p. 709, 2022.
39. M. O. Musa and T. Victor-Ime, "Improving Internet Firewall Using Machine Learning Techniques," American Journal of Computer Science and Technology, vol. 6, no. 4, pp. 170-179, 2023.
40. M. Nasir, N. A. Samsudin, W. Sharif, S. Baowidan, H. Arshad, and M. F. Mushtaq, "Towards Dimension Reduction: A Balanced Relative Discrimination Feature Ranking Technique for Efficient Text Classification (BRDC)," International Journal of Advanced Computer Science & Applications, vol. 15, no. 7, 2024.
41. M. R. Islam et al., "Leveraging advanced machine learning algorithms for enhanced cyberattack detection on US business networks," Journal of Business and Management Studies, vol. 6, no. 5, pp. 213-224, 2024.
42. A. Golduzian, "Predict And Prevent DDOS Attacks Using Machine Learning and Statistical Algorithms," arXiv preprint arXiv:2308.15674, 2023.