International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

ML-Powered Firewall for Adaptive Threat Detection and Real-Time Attack Prevention

Mrs. Priyanka Chandragiri[1], G. Subhash[2], K. Sujit Krishna[3], V. Teja[4]
[1]Assistant professor, Dept. of Cybersecurity, Malla Reddy University., Hyderabad, Telangana, India
[2,3,4]UG Scholar, Dept. of Cybersecurity, Malla Reddy University., Hyderabad, Telangana, India
Emails: *Priyach154619@gmail.com[1], Subhashgannapureddy1012@gmail.com[2], sujithkrishnakamarapu@gmail.com[3], Nagatejavadranam1453@gmail.com[4]*

Abstract
A largest number of interconnected ecosystems emerged from the quick spread of Network devices but this expansion has also left various environments susceptible to advanced cyberthreats especially network attacks. These attacks cause operational problems and pose serious security and privacy issues by taking advantage of flaws in networks. The complexity and scope of modern attacks are frequently beyond the scope of conventional detection techniques calling for sophisticated solutions that can effectively and precisely identify these dangers in real time. The hybrid machine learning approach was created in order to overcome these difficulties using the UNSW_NB15 dataset as a standard for examining network traffic data. To optimize feature selection and improve model performance many preprocessing techniques were used, such as standardization, feature encoding, Column Transformer, One Hot Encoder with chi-squared selection of features and Standard Scaler. Among the several machine learning models that were employed and evaluated Random Forest obtained an accuracy rate of 95%, Extra Trees 94.85%, the Decision Tree 93.69%, MLP 93.44%, Gradient boosting 93.15%, the KNN algorithm, 92.91% and Logistic Regression 91.07%. When it came to detecting seasonal patterns in network traffic the Long Short-Term Memory (LSTM) algorithm was the most effective with an accuracy in training of 96.665% and an accuracy in testing of 96.435%. Streamlit was used to create a simple user interface that lets users submit CSV data files with network traffic providing real-time attack alert system.

Keywords: *Attack Detection, Feature Selection, Hybrid Model, LSTM, Machine Learning, Preprocessing and UNSW_NB15.*

1. Introduction
Traditional security measures are failing to keep up with the latest attack methods in the contemporary digital environment, where security risks are growing more frequent and sophisticated [1]. Because they filter hostile traffic and stop illegal connections, firewalls have traditionally been the initial line of protection against cyber threats and illegal access. However, traditional rule-based firewalls are inefficient against advanced persistent threats (APTs), polymorphic malware and zero-day exploits because they mostly rely on static rules that have already been established and based on signatures identification techniques [2]. This calls for a clever, adaptable method regarding network security one which can identify trends, foresee possible dangers and adjust in real time to successfully reduce risks. Firewalls with machine learning (ML) capabilities overcome these constraints by using AI-driven algorithms to automatically identify, categorize and eliminate security breaches. ML-based firewalls improve the effectiveness of cybersecurity architecture [3] by continually gaining knowledge from system activity and adjusting to new threats. While static criteria and signature-based detection

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

methods are the foundation of traditional firewalls, they are unable to offer strong protection against constantly changing cyberthreats. In contemporary security designs, packet-filtering antivirus programs, stateful examination firewalls, virtual firewalls and next-generation firewalls (NGFW) are frequently employed [4]. Although these systems have advanced, they still mostly rely on pre-established security rules and rule sets, which leaves them open to new threats that don't fit the signatures that are currently in place. Furthermore, by keeping an eye on network traffic and spotting questionable activity, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) support firewalls. Conventional IDS/IPS solutions on the other hand produce a lot of false positives, flooding security teams with warnings that might not necessarily be indicative of real threats. The rising complexity and regularity of attacks which surpass the capabilities of conventional security measures, is the driving force behind the development of an ML-powered firewall [5]. As the use of cloud computing, IoT devices and remote job settings have grown in popularity, networks are now more susceptible to cyberattacks that take advantage of flaws in current security architectures. Human mistake occurs when firewall rules are configured and updated manually, which could result in security flaws. Furthermore, attackers use AI-driven tactics to initiate increasingly complex cyberattacks which calls for an antivirus system that is just as intelligent. The requirement for an adaptable safety device that can automatically identify anomalies, evaluate traffic in real time and take preventive action is a major driving force. Security teams may improve detection accuracy, decrease reaction times, and increase network resilience by incorporating machine learning (ML) into firewall architectures [6].

2. Literature Survey

A great deal of research has been conducted recently to address the increasing danger of network assaults in network firewall scenarios using state-of-the-art deep neural networks and machine learning techniques. Early approaches mostly relied on traditional machine learning approaches like Support Vector Machines (SVM), Random Forests and Decision Trees to extract patterns from static network data. When researchers investigated feature selection techniques including reciprocal data and chi-square to identify significant attributes influencing attack identification, the effectiveness of these algorithms was improved. A machine learning method for spotting malware networks in network traffic is presented by Salih et al. SVM and LR techniques are used in the method which shows promise in identifying firewall attacks [7]. Feature selection is an effective technique to improve classification accuracy while using less storage and processing power. Its uncertain polynomial-time hardness is well-known, nevertheless [8]. The feature selection techniques [9] employed in neural network-based attack detection models are thoroughly understood in this paper which also offers suggestions for enhancing these methods and points out areas in need of development. Jones et al. investigated the use of convolutional and recurrent neural networks (CNNs) for identifying attacks operations on networking. The models are more accurate and precise than conventional techniques [10]. However growing attacks and computing demands present difficulties. Models should be adapted for various IoT applications in future studies. Using multi-layer neurons and LSTM auto encoders, Ali et al. present an advanced learning hybrid method for detecting assaults in network systems [11]. According to Han et al., the Internet of Things or IoT has increased cyberattacks and transformed automation, necessitating a study of network analysis. This study suggests a methodology for analyzing IoT device communications that makes use of ensemble methods and supervised learning [12]. Due to its ability to effectively analyze spatial and sequential data, deep learning-based methods in particular Long Short-Term Memory (LSTM) and neural networks using convolution have gained popularity recently. The LSTM models especially have become more popular due to their ability to detect time patterns in network data [13]. This allows for more precise identification of changing network activity. Hybrid frameworks that combine deep learning models with conventional machine learning have showed promise in providing a compromise between predictive accuracy and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

computational efficiency. It focusses on the use of graph-based representations of communication records in firewall and intrusion detection [14]. A recent study recommends a multi-stage feature selection and computational weighted technique [15] for identifying a range of security threats in IoT networks. Krishnan et al. presented this method to address the issue of uneven attack classes and reduce cost in machine learning models.

3. Data Collection & Preprocessing

In order to analyze the activity occurring on connected devices and detect firewall attacks our study employed the UNSW_NB15 collection as a comprehensive benchmark [16]. This dataset is extremely relevant for assessing network security solutions because it was created using a complex network simulation system that includes current attack scenarios. Nearly 2.54 million records of computer network data make up this collection which includes both benign and malicious operations like backdoors, denial of service exploits and surveillance. A combination of basic traits, content-driven features, related to time characteristics and traffic-based statistics data are among the 49 aspects that enhance the dataset. In order to prevent characteristics with different sizes and units from excessively impacting the machine learning models normalization was an essential preprocessing step. This procedure improved model performance while maintaining the links between data points by converting all numerical attributes into a consistent range usually between 0 and 1. Normalization [17] increased training resolution rates and guaranteed optimal performance of distance-based algorithms like KNN and Decision Trees by scaling down big numerical quantities. In order to manage categorical data in the UNSW_NB15 dataset non-numerical attributes were transformed into numeric representations using feature encoding approaches. Depending on the circularity of the categorical variables a combination of One hot and Label encoding [18] was used. Label Encoding gave each category a unique integer value for characteristics with a finite number of distinct values. One hot Encoding was employed for high cardinality features producing binary cells for every unique category. These encoding techniques insured that the models could handle the data efficiently without adding skew by preserving the semantic significance of category information while making it readable by machines. In order to reduce dimensionality and increase the model computational efficiency feature selection was essential. The most appropriate characteristics for attack detection were found using the Select Best approach [19] in combination with the chi-squared (chi^2) statistical analysis (as shown in Figure1).

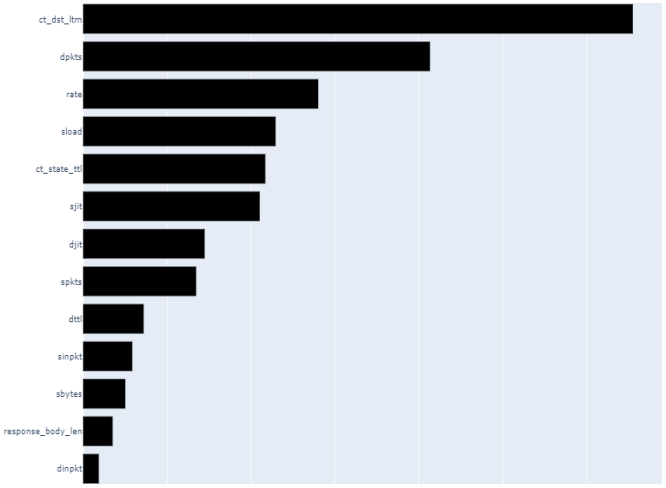

Figure 1 Top Features of UNSW_NB15 Dataset

A Column Transformer was used to perform particular transformations to several subsets of columns at once in order to speed up the preprocessing workflow. Preprocessing methods like normalization to numerical parameters and encoding to categorical characteristics might be used with ease within a single framework. The Column Transformer decreased the possibility of human error during data preparation and ensured integrity by automating these transformations. This approach also improved scalability making it possible to handle big datasets like UNSW_NB15 effectively without affecting preprocessing speed or accuracy. In order to further purify the information before putting it into the LSTM model the Standard Scaler [20] was included as the last preprocessing step. In order to maximize the data for gradient-based optimization approaches that are essential to deep learning systems, Standard Scaler standardized features by taking the mean and scaling these to unit variance.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

4. Principles and Methods

4.1 Random Forest

The Random Forest method of ensemble learning [21] uses many decision trees to improve the general accuracy of machine learning models particularly in tasks like classification and regression. A collection of decision trees is constructed during training and each tree's class or value corresponds to a majority vote (for grouping) or the mean estimate (for regression). Random Forest's ability to handle large, complex datasets such as the UNSW_NB15 dataset and its resistance to overfitting make it a valuable tool for detecting network attacks.

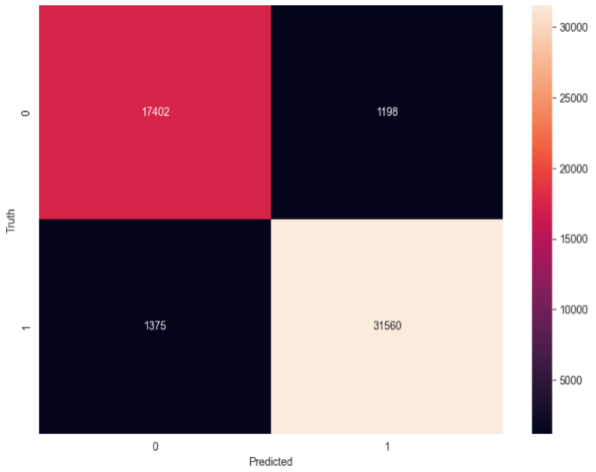

Figure 2 Confusion Matrix of Random Forest

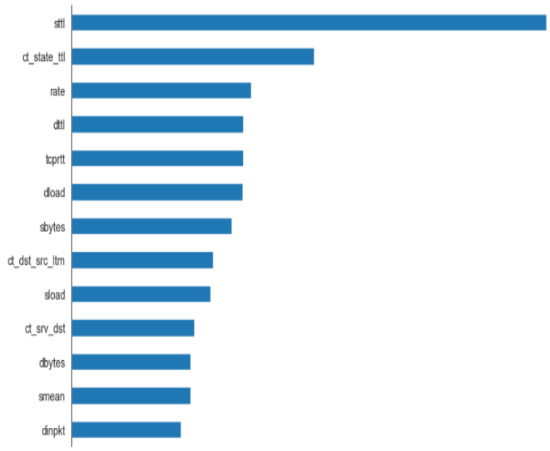

Figure 3 Feature Importance of Random Forest

One of Random Forests main benefits is its feature importance analysis capability which helps in determining which variables have the biggest influence on the forecast and offers insights into how network traffic behaves. This is done by a technique known as feature bagging in which a random selection of features is used to train each tree in the forest. In real world cyber scenarios, where network traffic is frequently noisy and contains useless information Random Forest is perfect since it is less dependent on noisy data and outliers. Compared to individual models Random Forest offers a more generalizable solution by averaging the predictions from multiple trees improving the detection of firewall attacks across a variety of networks and devices (as shown in Figure 2). The model's performance in this field is demonstrated by its high 95% detection accuracy of firewall traffic in this investigation (as shown in Figure 3).

4.2 Extremely Randomized Trees

Similar to Random Forest the ensemble learning method Extra Trees makes predictions using numerous decision trees but it builds these trees differently[22]. The decision trees of Extra Trees are constructed with a greater degree of randomization in both feature selection and feature split point determination. Extra Trees create even more randomized tree structures by randomly choosing a threshold for each characteristic and splitting the data in accordance with that threshold rather than choosing the optimal split based on some criterion.

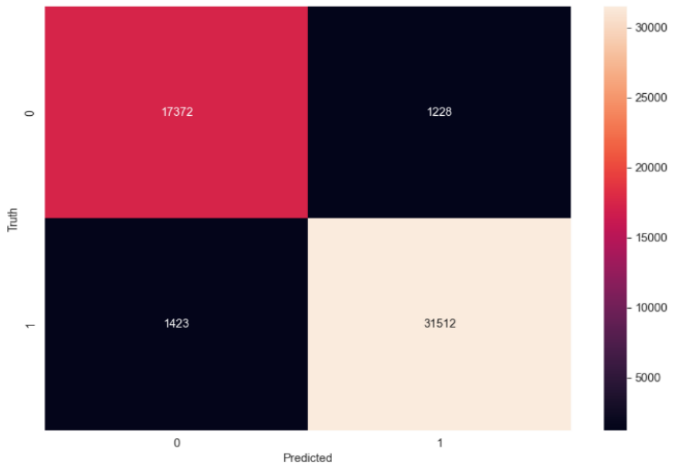

Figure 4 Confusion Matrix of Extra Trees Classifier

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

The major advantage of Extra Trees resides in its performance and speed particularly when dealing with massive data sets. By reducing the requirement for heavy optimization of each tree (such as determining the optimal split) Extra Trees can create trees faster making it an attractive solution for real-time detection situations. Extra Trees frequently outperform conventional ensemble techniques like Random Forest particularly in terms of precision and robustness, despite the extra randomness. Extra Trees remarkable 94.85% detection accuracy of network activity (as shown in Figure 4) in this investigation shows how well it can differentiate between benign and harmful cyber network data.

4.3 Decision Tree

A decision tree is a simple machine learning technique that iteratively splits the information set into subsets based on feature values, ultimately forming a tree-like structure where each node represents a feature and each branch indicates a decision rule [23]. Decision trees can be very helpful in the area of attack identification since they provide straightforward criteria for dividing network information into two categories: benign or malicious. The system chooses the most useful characteristics to divide the data based on parameters like information gain or Gini impurity which enables it to separate and spot patterns linked to attacks by firewall in cyber environments.

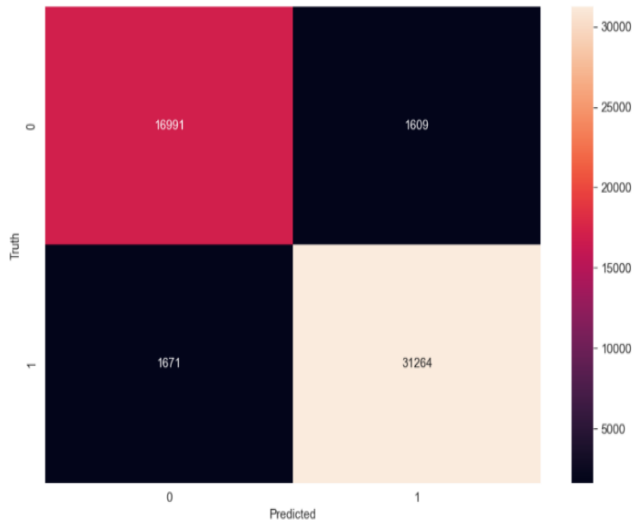

Figure 5 Confusion Matrix of Decision Tree Classifier

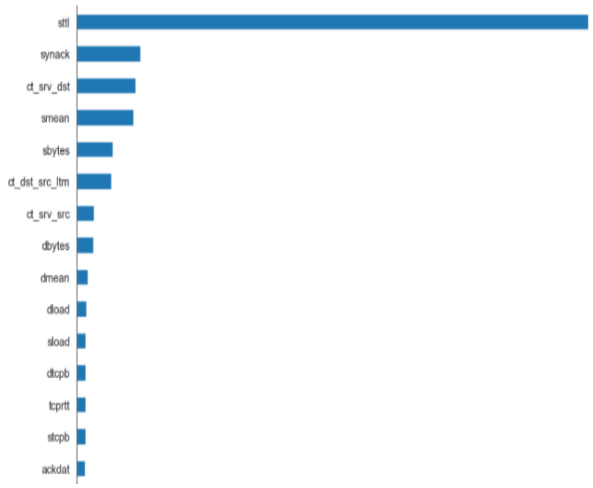

Figure 6 Feature Importance of Decision Tree

Because decision trees can handle numerical as well as categorical information and are highly computationally efficient despite their propensity for overfitting, they are adaptable for real-world datasets. Decision trees one of the foundational models for identifying attacks in this study identified malicious network traffic with a reasonable accuracy of 93.69% (as shown in Figure 5). This accuracy shows how well the system can identify patterns in traffic or irregular patterns that point to network activities. The introduction of ensemble techniques like Random Forest and Extra Trees which solve the overfitting problem while maintaining high accuracy also improves the performance of decision trees in the hybrid model. Furthermore, the comprehension and simplicity of the model are further improved by decision trees capacity to offer feature importance insights, which improve a deeper comprehension of the network attributes are most important in identifying firewall traffic (as shown in Figure 6).

4.4 Multilayer Perceptron

A feedforward ANN having several layers of neurons each completely connected to the next is called a multilayer perceptron (MLP) [24]. MLPs are strong machine learning algorithms that are especially well-suited for applications like firewall attack identification in cyber networks because they can capture complex non-linear correlations between input variables and target outputs. Usually, the architecture consists of an output layer that offers the final prediction one or more hidden layers that carry

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

out weighted shifts and an input layer that collects the features. MLP was used in this study to classify network information as either malicious or normal taking advantage of its capacity to represent complex connections and patterns that more simple algorithms such as decision trees might overlook.

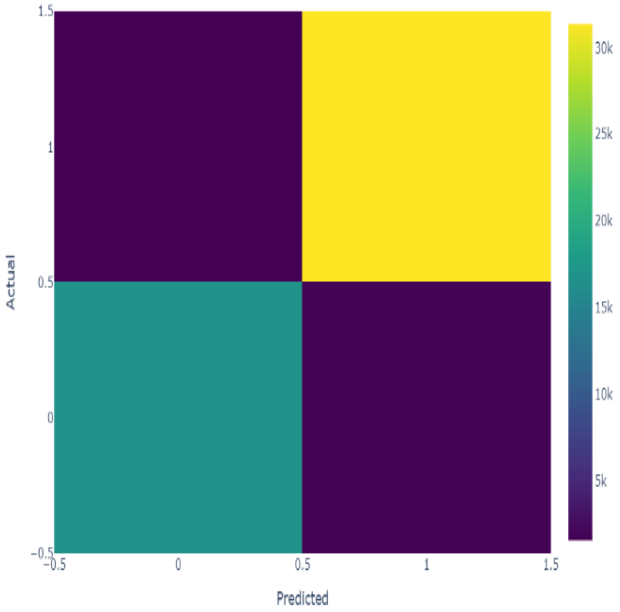

Figure 7 Confusion Matrix of MLP

MLPs require a lot of data and training time making them physically more demanding than typical machine learning models considering their strong capabilities. In this study MLP demonstrated its ability to discern between harmful and benign traffic by identifying attack incidents in the UNSW_NB15 dataset with an accuracy of 93.44% (as shown in Figure 7).

4.5 Gradient Boosting

A sophisticated ensemble learning technique called gradient boosting builds models one after the other with every additional model seeking to correct the flaws of the one before it [25]. By concentrating on the remaining mistakes from previous models Unlike conventional methods that create distinct models separately gradient boosting combines weak learners, usually decision trees into a potent prediction model. Through this repeated process the algorithm gradually improves prediction accuracy by learning from the errors of earlier trees.

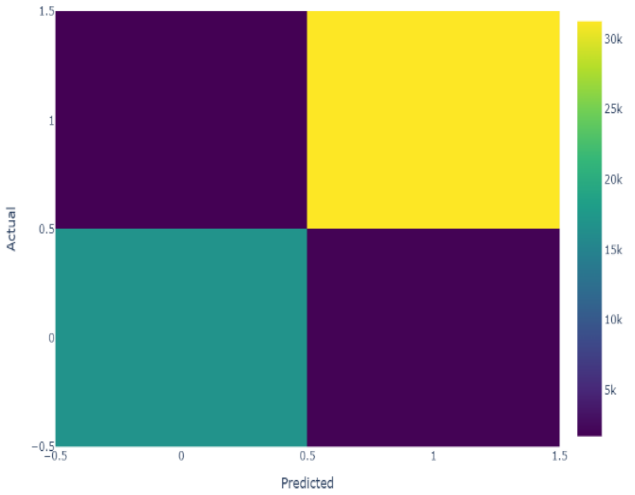

Figure 8 Confusion Matrix of Gradient Boosting

However, when there are too many trees or the model is too complicated gradient boosting may be prone to overfitting and noisy data. By using strategies like cross-validation and grid search hyperparameters like learning rate, maximum tree depth and number of estimators are carefully adjusted to reduce these problems. Gradient Boosting showed its efficacy in cyber safety applications in this study by detecting firewall attacks within the UNSW_NB15 dataset with an accuracy of 93.15% (as shown in Figure 8).

4.6 K-Nearest Neighbors

K Nearest Neighbors (KNN) is a straightforward non-parametric machine learning technique that clusters data points in the feature space based on the vast majority class that are their closest neighbors[26]. After calculating the distance among the test point and another point in the training data set it allocates a test point to the class with the highest relevance among its closest neighbors. However, because the approach requires determining the distance between the tested point and every other point in the dataset one of the primary disadvantages of KNN is its computing inefficiency particularly when working with big datasets like the UNSW_NB15 dataset. Slower prediction rates and more memory usage may result in real time systems for detection. Furthermore, KNN accuracy and performance can be affected by the parameter k and the distance metric (such as Manhattan or Euclidean) that are used. Considering these drawbacks KNNs

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

92.91% accuracy rate in the study showed how useful it is for identifying firewall attacks in cyber traffic (as shown in Figure 9).

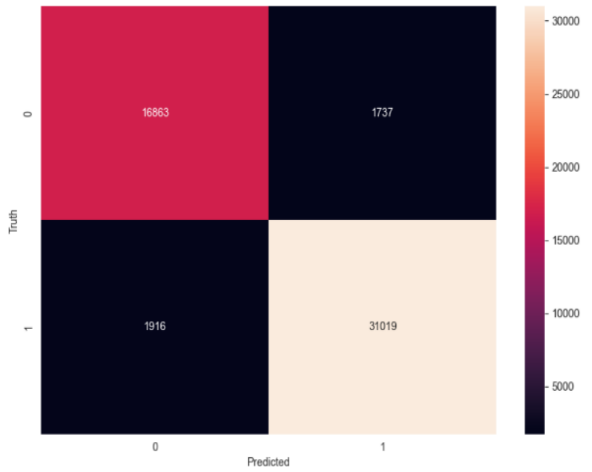

Figure 9 Confusion Matrix of KNN Classifier

4.7 Logistic Regression Classifier

Logistic regression is a statistical method for tasks involving binary classification[27] that predicts the likelihood that a given instance will fall into a particular class by examining the relationship between the input information and the desired variable using a function called logistic. In the context of attack detection in cyber environments network traffic is classified as either beneficial or destructive using logistic regression. The model is a simple but effective method for performing binary classifications when the basic connection across the attributes and the result is approximately linear. It operates by fitting a linear boundary for decisions between the two classes. Despite its benefits logistic regression is not always able to handle intricate connections and non-linear information which are frequently present in network traffic. In these situation s attack patterns are frequently more complex and challenging to distinguish using the linear decision boundary. Although it placed behind alternative models like Random Forest and Extra Trees logistic regression demonstrated its capacity to differentiate between harmful and genuine traffic in this study by detecting network activities within the UNSW_NB15 dataset with an accuracy of 91.07% (as shown in Figure 10).

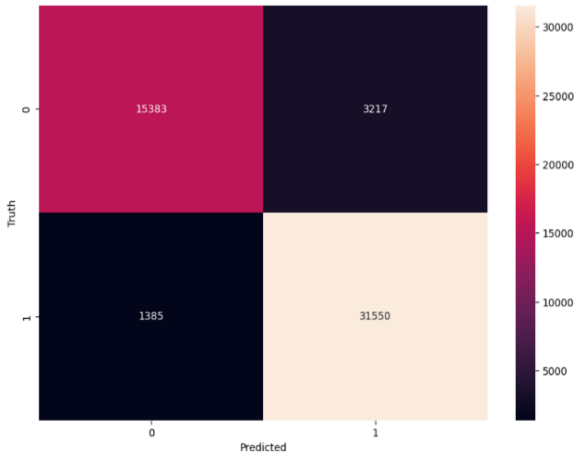

Figure 10 Confusion Matrix of Logistic Regression

4.8 Long Short-Term Memory

Long Short-Term Memory (LSTM) a unique type of recurrent neural network (RNN) designed to handle sequential data is incredibly helpful for applications needing analysis of time-series or additional information where the order of inputs matters [28]. Because network activity frequently changes over time in attack detection LSTM's capacity to identify these relationships over time allows it to identify minute long-term trends in the data that may point to a firewall attack. A number of essential elements make up the LSTM design which sets it apart from conventional RNNs [29]. It has three entry points: the input gate, the forget gate and the output gate. Data storage is the responsibility of the memory cell. The input gate determines which information from the present input is stored in the memory cell (as shown in Figure 11). The forget gate decides what information should be deleted from the cell's previous state, while the output gate regulates what information is transferred from the memory cell to the layer below. By addressing the vanishing gradient issue these gates enable LSTM to retain dependence over time without gradually losing relevant information. After then the model gains knowledge from these characteristics identifying patterns of both typical and unusual conduct that change over time [30].

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

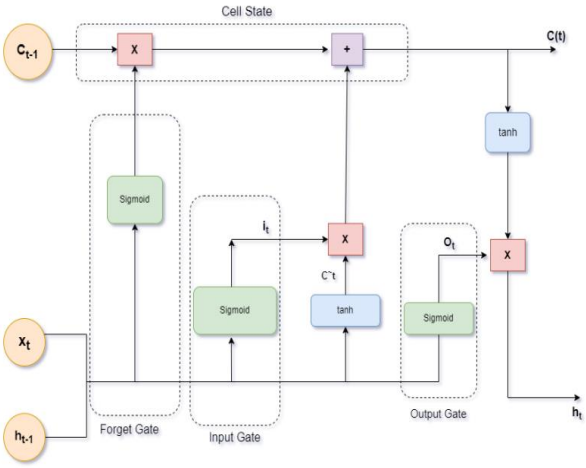

Figure 11 LSTM Layer Architecture

Figure 12 Training and Testing Accuracy of LSTM

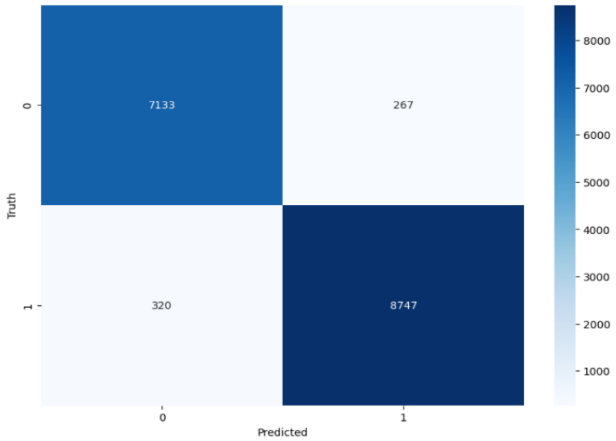

Figure 13 Confusion Matrix of LSTM Network

In order to help with prediction based on learnt features LSTM is sometimes integrated by adding extra layers such as a dense output layer for classification. The model's capacity to identify firewall attacks can be further improved by adding dropout regularity or bidirectional LSTMs which gather data from both previous and next time steps. The LSTM model showed remarkable performance in this study with a Training Accuracy of 96.665% and a Testing Accuracy of 96.435% (as shown in Figure 12). This high accuracy shows how well LSTM captures the complex and continuously shifting nature of attacks in cyber environment. In contrast to conventional machine learning models which could find it difficult to identify attacks with changing patterns LSTM (as shown in Figure 13) is highly skilled at recognizing dependence over time.

5. Results

The efficiency of the strategy was demonstrated by the remarkable outcomes of the machine learning algorithms used to the UNSW_NB15 dataset for firewall attack detection. Random Forest had the best accuracy of 95% out of all the machine learning models that were evaluated. Extra Trees, Decision Tree and MLP came in second and third respectively with 94.85%, 93.69%, and 93.44%. The best accuracy was 93.15% for Gradient Boosting 92.91% for KNN, and 91.07% for Logistic Regression. But with a remarkable Training Performance of 96.665% and Testing Accuracy of 96.435% the Long Short-Term Memory (LSTM) model outperformed the others by significantly making it the best model for identifying firewall attacks in cyber situations (as shown in Figure 14). The best-performing approach LSTM has been further verified for its improved performance by the confusion matrix. While the false positive rate was comparatively low ensuring that real traffic was not mistakenly divided as malicious the matrix shows a high true positive rate suggesting that the model successfully detected firewall attacks. Because it performed well in both the training and testing phases and produced few wrong classifications the LSTM model is an accurate option for actual time attack identification. LSTM excelled more conventional machine learning models in terms of accuracy

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

because it was able to identify delicate patterns of attacks that other models might have overlooked because to sequential learning and its ability to identify relationships that last in the data (as shown in Figure 15 & 16). Moving on to real-time analysis the attack detection system gained greatly from the deployment of a Streamlit-based user interface which offered a platform for rapid and dynamic analysis (as shown in Figure 17).

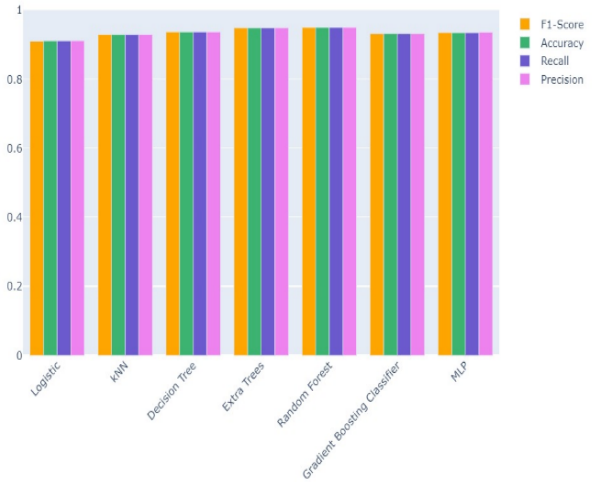

Figure 14 Comparison of Machine Learning Classifiers

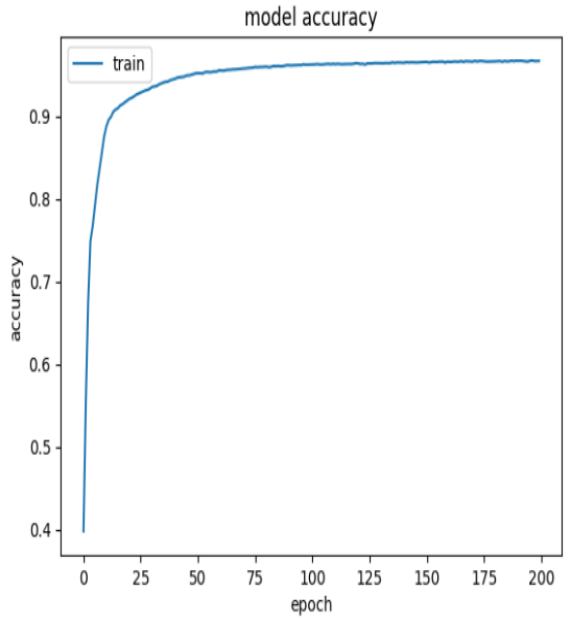

Figure 15 LSTM Accuracy Plot vs Epochs

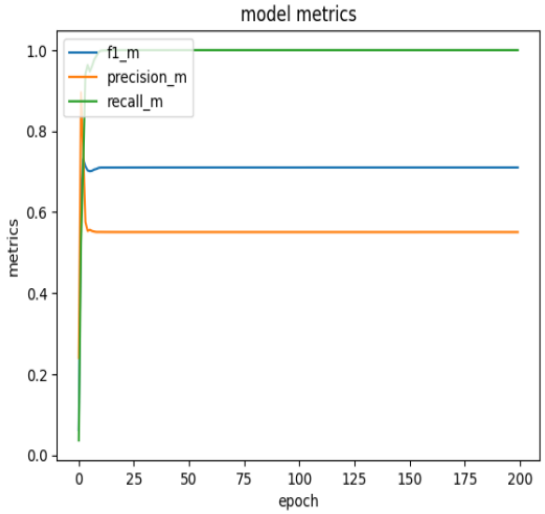

Figure 16 Performance Metrics of LSTM Model

The system is ideal for implementation in real time cyber scenarios where prompt detection and reaction are essential since it delivers actionable findings in real time. The system is a readily available instrument for safety professionals and administrators since it enables simple involvement and provides instant response. The real-time system not only classifies observed firewall activity but also offers preventive measures. The system recommends particular steps to reduce the threat if an automated network attack is identified such blocking dubious IP addresses, screening traffic or looking into unusual patterns further. In order to prevent possible harm from evolving firewall attacks the real-time monitoring module considers both the current network context and the traffic pattern over time.

Figure 17 Sample Data of CSV for Attack Detection

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

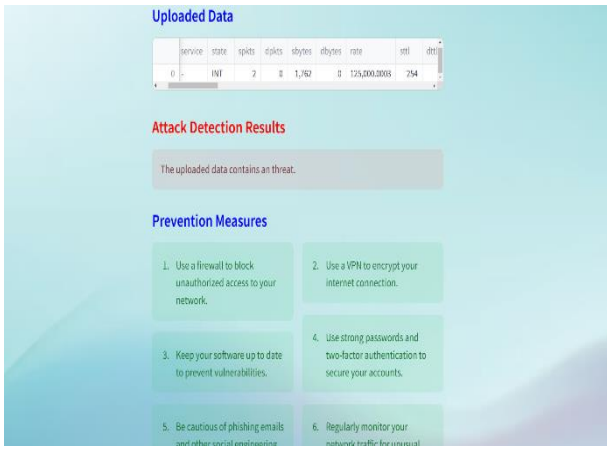

Figure 18 Firewall Attack Detection

With the help of streamlit's user-friendly interface users may upload data files and get results right away in a simple and efficient manner. In situations where time is of the importance this usability is especially crucial. Detailed visualizations of detection results such as graphs displaying traffic patterns, attack categories, give alerts and recommended preventive measures are available to administrators (as shown in Figure 18).

Conclusion

This study provides a sophisticated hybrid machine learning framework for efficient firewall attack detection in cyber environments by utilizing a range of models, such as Random Forest, Extra Trees, Decision Tree, MLP, Gradient Boosting, KNN, Logistic Regression and LSTM. It highlights particularly on LSTM's exceptional ability to record time changes in network activity data. With LSTM outperforms other models the suggested approach achieves remarkable accuracy proving its capacity to identify subtle and changing network patterns of attack in cyber contexts. With the help of the real-time detection technology and an intuitive streamlit interface network traffic can be processed and evaluated instantly giving managers useful information, gives alerts and preventative actions to reduce dangers. The system is a useful tool for protecting firewall networks from advanced ongoing cyber threats because of its real-time attack detection and prevention capabilities, strong accuracy and effective computational performance. The promise of machine learning and deep learning approaches in improving network security strategies is highlighted by this hybrid strategy which when paired with real-time prevention capabilities provides a holistic solution to the increasing issues in IoT cybersecurity.

References

[1]. Aslan, Ömer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12.6 (2023): 1333.

[2]. Niu, Gang, Xun Dong, and Yuejian Chen. "Motor fault diagnostics based on current signatures: A review." IEEE Transactions on Instrumentation and Measurement 72 (2023): 1-19.

[3]. Nayar, Vinayak, et al. "Optimizing Real-Time Performance in ML-Based Application Layer Firewalls." International Conference on Cognitive Computing and Cyber Physical Systems. Singapore: Springer Nature Singapore, 2023.

[4]. Sichkar, Mykhailo, and Larysa Pavlova. "A short survey of the capabilities of Next Generation firewalls." Computer Science and Cybersecurity 1 (2023): 28-33.

[5]. Lasantha, NW Chanka, et al. "Validating IP Reputation in Cloud Firewall Systems Using Machine Learning Driven Signature Generation and Detection Techniques." 2024 IEEE Industrial Electronics and Applications Conference (IEACon). IEEE, 2024.

[6]. Ahmadi, Sina. "Next generation ai-based firewalls: a comparative study." International Journal of Computer (IJC) 49.1 (2023): 245-262.

[7]. Salih, Yousif Tareq, et al. "Machine Learning Approaches for Botnet Detection in Network Traffic." Proceedings of the Cognitive Models and Artificial Intelligence Conference. 2024.

[8]. Baruah, Sangita, Dhruba Jyoti Borah, and Vaskar Deka. "Reviewing various feature selection techniques in machine learning-based botnet detection." Concurrency and Computation: Practice and Experience 36.12 (2024): e8076.

[9]. Theng, Dipti, and Kishor K. Bhoyar. "Feature selection techniques for machine learning: a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

survey of more than two decades of research." Knowledge and Information Systems 66.3 (2024): 1575-1637.

[10]. Jones, Rebet Keith. "Enhancing IoT Security: Leveraging Advanced Deep Learning Architectures for Proactive Botnet Detection and Network Resilience." Redefining Security with Cyber AI. IGI Global, 2024. 56-71.

[11]. Ali, Shamshair, et al. "A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks." Alexandria Engineering Journal 103 (2024): 88-97.

[12]. Han, Seung-Ju, Seong-Su Yoon, and Ieck-Chae Euom. "The Machine Learning Ensemble for Analyzing Internet of Things Networks: Botnet Detection and Device Identification." CMES-Computer Modeling in Engineering & Sciences 141.2 (2024).

[13]. Al-Selwi, Safwan Mahmood, et al. "RNN-LSTM: From applications to modeling techniques and beyond—Systematic review." Journal of King Saud University-Computer and Information Sciences (2024): 102068.

[14]. Lagraa, Sofiane, et al. "A review on graph-based approaches for network security monitoring and botnet detection." International Journal of Information Security 23.1 (2024): 119-140.

[15]. Krishnan, Deepa, and Pravin Shrinath. "Enhancing energy efficiency and imbalance handling in botnet detection in IoT networks: a multi-stage feature reduction and weighted approach." International Journal of Information Technology (2024): 1-12.

[16]. Jouhari, Mohammed, Hafsa Benaddi, and Khalil Ibrahimi. "Efficient Intrusion Detection: Combining X 2 Feature Selection with CNN-BiLSTM on the UNSW-NB15 Dataset." 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2024.

[17]. Fujita, Takaaki. "A review of fuzzy and neutrosophic offsets: Connections to some set concepts and normalization function." Advancing Uncertain Combinatorics through Graphization, Hyperization, and Uncertainization: Fuzzy, Neutrosophic, Soft, Rough, and Beyond 74 (2024).

[18]. Williams, Christopher KI. "Naive Bayes Classifiers and One-hot Encoding of Categorical Variables." arXiv preprint arXiv:2404.18190 (2024).

[19]. Maftoun, Mohammad, et al. "Improving Prediction of Mortality in ICU via Fusion of SelectKBest with SMOTE Method and Extra Tree Classifier." International Work-Conference on the Interplay Between Natural and Artificial Computation. Cham: Springer Nature Switzerland, 2024.

[20]. Thakker, Zalak L., and Sanjay H. Buch. "Effect of Feature Scaling Pre-processing Techniques on Machine Learning Algorithms to Predict Particulate Matter Concentration for Gandhinagar, Gujarat, India."

[21]. Sun, Zhigang, et al. "An improved random forest based on the classification accuracy and correlation measurement of decision trees." Expert Systems with Applications 237 (2024): 121549.

[22]. Baldini, Gianmarco. "Mitigation of Adversarial Attacks in 5G Networks with a Robust Intrusion Detection System Based on Extremely Randomized Trees and Infinite Feature Selection." Electronics 13.12 (2024): 2405.

[23]. Sun, Zhigang, et al. "An improved random forest based on the classification accuracy and correlation measurement of decision trees." Expert Systems with Applications 237 (2024): 121549.

[24]. Naseer, Aysha, and Ahmad Jalal. "Multimodal Objects Categorization by Fusing GMM and Multi-layer Perceptron." 2024 5th International Conference on Advancements in Computational Sciences (ICACS). IEEE, 2024.

[25]. Esmaeili-Falak, Mahzad, and Reza Sarkhani Benemaran. "Ensemble extreme gradient boosting based models to predict the bearing capacity of micropile group." Applied Ocean Research 151 (2024): 104149.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1398-1409
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0199

[26]. Halder, Rajib Kumar, et al. "Enhancing K-nearest neighbor algorithm: a comprehensive review and performance analysis of modifications." Journal of Big Data 11.1 (2024): 113.
[27]. Das, Abhik. "Logistic regression." Encyclopedia of Quality of Life and Well-Being Research. Cham: Springer International Publishing, 2024. 3985-3986.
[28]. Louis, F. "Long Short-Term Memory (LSTM) Networks." (2024).
[29]. Waqas, Muhammad, and Usa Wannasingha Humphries. "A critical review of RNN and LSTM variants in hydrological time series predictions." MethodsX (2024): 102946.
[30]. Boddapati, Mohan Sai Dinesh, et al. "Creating a Protected Virtual Learning Space: A Comprehensive Strategy for Security and User Experience in Online Education." International Conference on Cognitive Computing and Cyber Physical Systems. Cham: Springer Nature Switzerland, 2023.