Design Secure Authentication Methods to Prevent Unauthorized Access to Critical Systems and Networks

Tharun D, V. Madhu Sudhan , C. Hemalatha and Abirami G
Department of Computer Science & Engineering, Sathyabama University, Chennai, Tamil Nadu, India

Keywords: Network Security, Machine Learning (ML), Intrusion Detection, Stacking Classifier, UNSW-NB15 Dataset, Cyber Threats.

Abstract: As cyber threats become increasingly more complex, securing the communication of network communication is a major challenge. One of the reasons for that is that traditional security measures are not able to adjust with constantly changing attack tactics, thus, it is necessary to incorporate ML driven approaches to improve network security. In this research study, we examine the efficiency of different ML model for handling malicious activities in network traffic employing UNSW-NB15 dataset. NS-LR, NS-SVM, NS-KNN, NS-MLP, NS-GBM and a Stacking Classifier is applied for comparison with each other. A complete feature correlation analysis and multiple class classification is conducted to evaluate the model performances with a aid of metrics as accuracy and AUC-ROC. The conducted results show Stacking Classifier's superiority over other models with near perfect accuracy that determines it as a good choice for real time network intrusion detection systems. In contrast, MLPs limited the classification performance and led to additional training needed. This work demonstrates the feasibility of application of ML driven schemes for the protection of contemporary networks against highly sophisticated cyber attacks. The inclusion of adversarial learning techniques and the integration with explainable AI (XAI) towards real time deployment will then be taken as future work.

1 INTRODUCTION

On present days, cyber threats have become so sophisticated that there is always threat to network security. The traditional security mechanisms including rule-based firewall and intrusion detection based on signatures are unable to cope with emerging attack pattern. At the same time, both cybercriminal techniques are getting increasingly more complex, and it has never been more important to have intelligent, adaptable security solutions than today.

ML has risen as a potentially hopeful method to assist in increasing the network security by identifying and countering the malicious incidents in real time. Unlike conventional methods, ML models are capable of learning patterns in network traffic data, and making highly effective at discovering known as well as unknown threats. In this study, using ML-based classification models, the ability of them to differentiate between normal and hateful traffic on network protocols is evaluated.

We compare a few ML models using the UNSW-NB15 dataset, that is a set of diverse types of cyber attacks, including L NS-LR, NS-SVM, NS-KNN, NS-MLP, NS-GBM and Stacking Classifier. Finally, the models are assessed with standard performance.

The foremost intent of this research entails to figure out the maximum promising ML model for network IDS and enhancing safekeeping with advanced classification techniques. We found that Stacking Classifier always outperforms other models on accuracy and detection rate. This confirms the good potential of the ensemble learning techniques for the implementation of robust real-time threat detection systems.

Previous works in this area could turn their attention to incorporating Explainable AI (XAI) technologies to improve interpretability, developing model efficiency for practical deployment, and also discovering ways to resist evolving cyber threats using adversarial learning. The work presented in this paper expands the emerging set of research on AI driven network security to show ML's radicalizing influence in preserving online infrastructure.

D., T., Sudhan, V. M., Hemalatha, C. and G., A.
Design Secure Authentication Methods to Prevent Unauthorized Access to Critical Systems and Networks.
DOI: 10.5220/0013908700004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 4*, pages 95-100
ISBN: 978-989-758-777-1

2 LITERATURE REVIEW

In the first place Liu, Tang and Qin analyze authentication challenges in software defined optical access networks where optical line terminals and optical network units are critically growing and it requires stronger security measures. In order to address these concerns, the authors propose a trivial two-way confirmation (LTWA) plan that makes use of the cryptographically generated tackle algorithm in conjunction with the confusion generated speak to algorithm. This approach provides secure end to end communication and stops attackers from forging authentication messages, proving their capacity of minimizing the risk of security in the optical networks.

In his et al, the secure access in the distributed power networks for IoT hub equipment is discussed to practice the security deficiency from the aspect of restricted resources of IoT device's. They suggest a simple two-way authentication approach using the SM algorithm with the help of digital signature and Diffie Hellman protocol. This approach they find to be effective at mitigating such network attacks as eavesdropping and tampering and thus suitable for real world IoT security applications.

In the IoT environment, Sharma and Babbar analyze the Increased threat of Android malware in the IoT environment and explore the use of ML algorithms for detecting malware. Afterwards, their study is compared different model and is able to conclude that Decision Tree classifier gives the best accuracy of 95% in detecting the malicious applications. However, the study proposes that ML based models can be used as security boosted method of IoT devices to fend off malware attacks.

Further on the work of machine malware detection with deep learning, Zhang, Zou and Zhu use DNN for Android malware detection. In this paper, they combine static behavioral feature extraction with dynamic behavioral analysis in order to improve classification accuracy. The study surpasses existing nonparametric machine learning such as LR and SVMs when using RNNs to detect malware patterns.

In a graph neural network (GNN) for malware detection, Wang et al introduce his approach. In their method, they embed call graphs of applications into a deep neural network (DNN) to represent relationship between calls. Traditional ML based classifier are strongly outperformed by our model, which reaches an accuracy of 97.7%. Results show that GNNs are effective in detecting malicious behaviors through the structural network analysis.

Pagan and Elleithy propose a multi layer security approach to tackling the threat of ransomware. Proactive defense in their framework includes firewalls, DNS/Web filtering, email security, backups and employee training. Traditional antivirus solutions are shown to have shortcomings in the study which suggest that more successful ways of avoiding ransomware secure from the first layer of defense.

A Fuzzy Learning Network for energetic movable Malware Detection was proposed by Martinelli, and Santone. Given their model combines fuzzy logic and deep neural networks, they are able to achieve high accuracy detection of zero-day threats. As an emphasis on the dynamic nature of the malware attacks, this research focuses on the field of hybrid AI techniques.

Mercaldo and Santone consider image-based malware detection with a deep-neuro-fuzzy model in another work. They evaluate over 20,000 real world malware samples and achieve 93.5% accuracy using the image-based classification approach achieving a promise of the potential of image-based classification in cybersecurity.

The work by Rohith and Kaur gives a complete review of malware detection and prevention techniques, including signature-based systems and machine learning based antivirus systems. Their research outlines the challenges associated with maintaining the momentum when new malware is continuously developing, and injects input about the need for adaptive forms of cybersecurity.

In this context, Mercaldo and Santone propose a proper post checking method for malware relations classification. They take to reduce redundant comparisons and provide a maliciousness metric that aids in increases in the efficiency of malware detection systems.

3 METHODOLOGY

A machine learning based network traffic analysis is proposed to implement the above malware detection system to classify the network traffic as either benign or malignant. The methodology involves various arguable stages such as data gathering, data processing, feature selection, train model, evaluate and finally deployment. This structured approach provides an ability for a scalable and efficient intrusion detection system that can-do real time threat identification.

In the first step, data is collected using UNSW-NB15 dataset as the main dataset. There are both normal and malicious network traffic data in this dataset. Fuzzers, Backdoors, Probabilistic Denial-of-Service, Exploits, Reconnaissance, and Worms are included as attack types in it, which provides an

effective means for the evaluation of intrusion detection models.

The data is then preprocessed before the dataset is collected as such increase the model efficiency. Data cleaning which involve removing missing values and duplicate entries to reduce influence of inconsistencies is what it means. Non-numeric ie protocol types and connection states are encoded into a number for the categorical data. Also, normalization is performed to eliminate the effect of size differences in features and prevent some of the features from being overly influential in determining model prediction. Then, correlation analysis is used to remove less significant attributes to reduce computational complexity but select only the most significant attributes.

The model training and evaluation phase includes the choice of a group of machine learning algorithms to be ensured robust for malware detection. And trained and assessed are the following models:

- Baseline Classifier for Binary Classification tasks is Logistic Regression. Since it is simple, it is well suited for initial analysis.
- Then I discuss K-Nearest Neighbors (KNN) for classifiying network traffic into known classes based on already observed instances. It is very useful for recognizing malwared variants that have similar behavior.
- An example of deep learning model is Multi Layer Perceptron (MLP) network for learning complex patterns such as network traffic which also can help us to detect the previously unseen malware threats.
- One used for its capability to work well with high dimensional data and set up optimal decision boundaries for malware classification is SVC.
- GBC is a cooperative learning model that consists of an elegant mechanism to sequentially correct the instances misclassified by its preceding classifier.

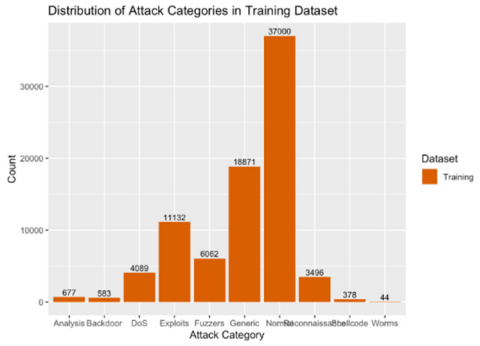

Figure 1: Distribution of attack categories in the training datasetz..

Contrary to the primitive neural network models that we used in this project (in the 'Application' section), each model is hyperparameter tuned using approaches like Grid Search to enhance the performance. The dataset is split into 80% train data and 20% test data to fairly evaluate the model's ability to simplify. The effectiveness of the proposed models is evaluated using key metrics to detect malware. Figure 1 show the Distribution of attack categories in the training datasets.

Then the best performing model is integrated into a Flask-based web application to be used for real time malware detection. In the deployment phase, the network traffic is monitored, and the system classifies the packets as either normal or malicious, at all times. It offers the Flask interface and gives ability to the network administrators to visualize threats detected and also take some security steps in the interactive dashboard. It also comprises a threat management module, to allow users to block or further investigate suspect traffic.

While the system was accurate, it has a few challenges, some of which include cases of adversarial attack, whereby attackers attempt to circumvent detection by changing their attack patterns. To solve this, future improvements will utilize adversarial learning techniques to enhance the models' robustness levels. Further, combining Explainable AI (XAI) will help explaining how predictions are made, which will give the cybersecurity professionals more transparency in the model decision making process. Federated Learning will be also implemented to empower distributed malware detection with a set of distributed organizations collaboratively training models without revealing data.

4 RESULTS

Different classification models were evaluated with respect to their ability of classifying malicious network activity. After test on UNSW-NB15 dataset, the performance in terms of classification accuracy and linear discriminant between normal and abnormal traffic of each model is measured.

4.1 Accuracy Comparison of Different Models

Figure 2 compares the overall precision of the various classification models. The outcome show that stacking classifiers are better than any other models tested, and achieved the highest accuracy. The stacking classifier utilises multiple models, whereby their predictions are

aggregately predicted in order to improve on robustness. On the other hand, the traditional models such as NS-LR, NS-SVM, and NS-KNN perform well except for a slight fall behind with the predictive performance. While the MLP and NS-GBM come out with relatively lower accuracy, it also points out that there is still a place to do the feature engineering and hyperparameter optimization.

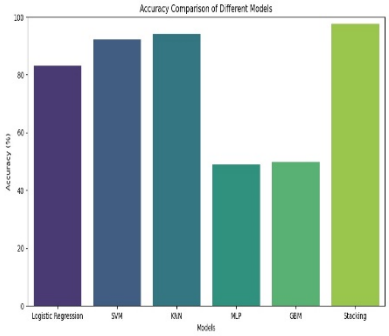

Figure 2: Accuracy Comparison of Different Models.

4.2 Data Distribution Analysis

For a better understanding of the dataset characteristics, a pie diagram presentation the particular circulation of standard and irregular labels is presented in Figure 3. In this the dataset is imbalanced; traffic which is normal constitutes 75.99 while the abnormal traffic constitutes 24.01. As indicated by this imbalance, it is necessary to use algorithms that generalize well across types of attack and are not biased towards the majority class.

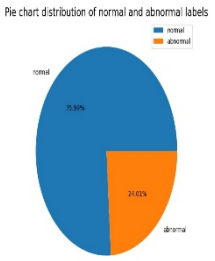

Figure 3: Chart of Standard and Irregular Label.

In particular, Figure 4 expands on this by showing the multi-class distribution of attack categories in the dataset, where one can observe that the dataset contains several attack types such as backdoors, fuzzers, reconnaissance, exploits, DoS, worms, and generic attacks. Normal traffic represents the greatest part of all (48.66%), while backdoor attacks are 24.01% and fuzzers 19.94%. Most of the other attack types are fairly rare.

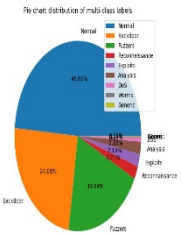

Figure 4: Chart of multi-class labels.

4.3 Feature Correlation Analysis

Interdependencies among the network traffic attributes are understandable by feature correlation. Figures 5 and 6 present correlation matrices for dual and multi-class labels, respectively. The different features can influence each other on the heatmap indicating how each of them may have contributed to attack classification.

- The binary correlation matrix (Figure 5) shows some strong correlation between certain traffic parameters indicating that there are some features that can tell more about attack behavior.
- This analysis is then furthered by expanding across multiple attack categories using the multi-class correlation matrix (Figure 6).

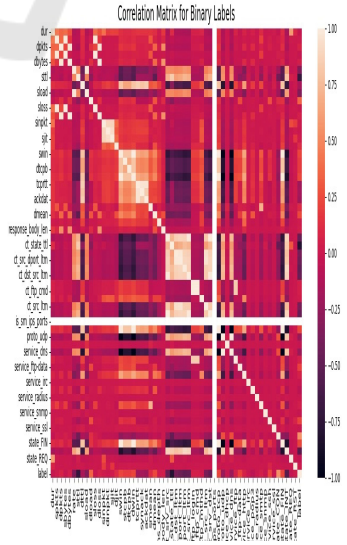

Figure 5: Binary Correlation Matrix.

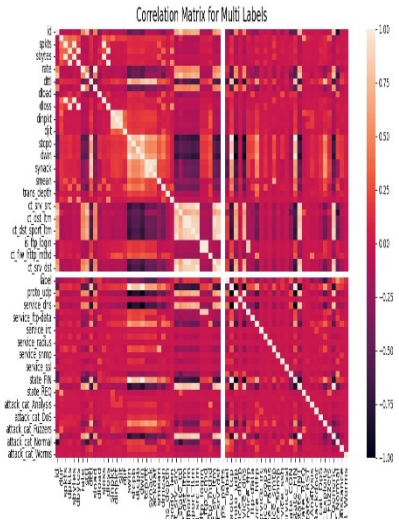

Figure 6: Label Correlation Matrix.

4.4 Model Performance Analysis

Different visualization methods are used to evaluate predictive performance of various classification models.

Logistic Regression Multi Class (Figure 7) Since NS-LR is a linear model, it is not easy to model curve like relationships. While it compares quite well relatively speaking, it's still less accurate than one of the ensemble learning techniques.

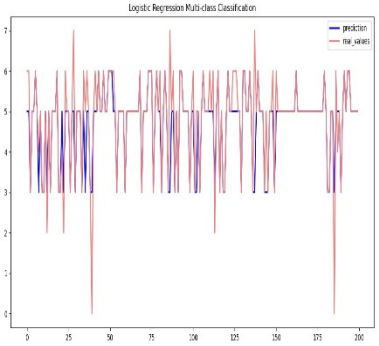

Figure 7: NS-LR Multi-Class Classification.

Linear NS-SVM Multi-Class Classification (Figure 8) While SVM is powerful in high-dimensional spaces, its effectiveness on the processed dataset is rather moderate. Although it accomplishes classification of some attack types, it is not adaptable for other nuances of attacks

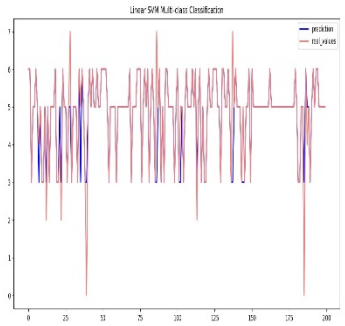

Figure 8: Linear NS-SVM Multi-Class Classification.

NS-KNN Multi-Class Classification (Figure 9) NS-KNN is computationally feasible when attacking data that has significant similarities being computed but is computationally expensive and infeasible when it runs in a large dataset.

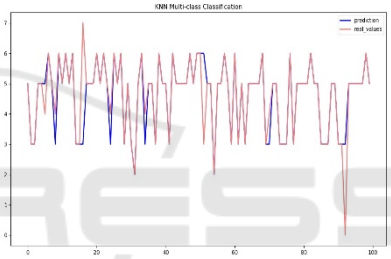

Figure 9: NS-KNN Multi-Class Classification.

NS-MLP Multi-Class Classification (Figure 10) However, the MLP model has its limitations in predicting the network traffic attacks which could be due to over fitting or poor hyperparameter tuning. This means that the model does not generalize well, where the predicted values stayed nearly flat.

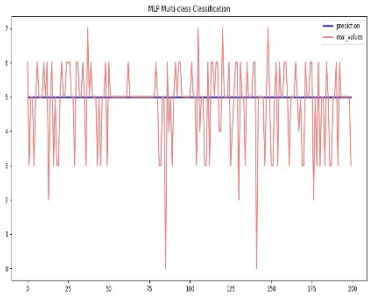

Figure 10: NS-MLP Multi-Class Classification.

NS-GBM Multi-Class Classification (Figure 11). Iterative learning is performed in order to reduce GBM's bias and variance, and thus leading to

improved performance. The prediction plot is fluctuating which means the model is refining itself while in classification.

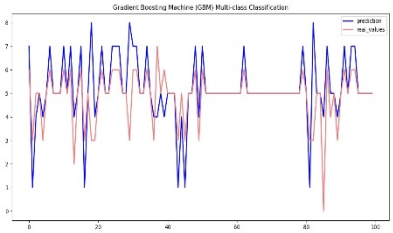

Figure 11: NS-GBM Multi-Class Classification.

ROC Curve for Multi-Class Stacking Classifier (Figure 12)

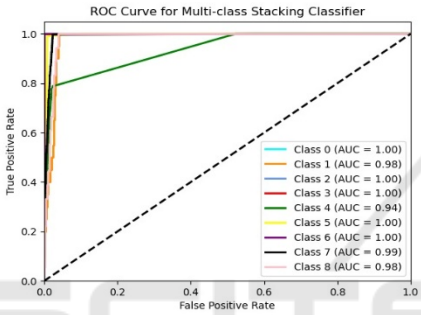

Figure 12: ROC Curve for Multi-Class Stacking Classifier.

Our results show that stacking classifier gives the best performance in the ROC curve with high AUC across domains of multiple attack categories. This model succeeds in differentiating among numerous types of malicious activities with values from 0.94 to 1.00.

5 CONCLUSION

Driven by the incredible increase of cyber threats, ML based IDS has the desire of providing a robust tool for detection of malicious behaviors. While this study focuse on maximizing the performance of a variety of multiple classification models to detect malicious network activity on UNSW-NB15 dataset. There are a number of key insights that resulted from extensive evaluation and performance analysis. Amongst all, the stacking classifier gave the highest accuracy when combined with the predictions of multiple classifiers unlike the traditional machine algorithms. According to the ROC curve, the stacking method comes close to 1.0 of AUC and can distinguish between normal and abnormal traffic with great precision. Models like the Logistic Regression and SVM also performed moderately, but MLP for its part never was good at predicting stably and required more tuning of the hyperparameters.

REFERENCES

T. Liu, Y. Tang, and P. Qin, "Security authentication based on generated address algorithm for software-defined optical communication network," *IEEE Access*, vol. 7, pp. 142673–142684, 2019.

B. He, B. Zhang, L. Zhang, Z. Xi, Y. Fang, and Y. Wang, "A lightweight IoT terminal authentication method based on the SM algorithm," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 1, pp. 112–125, 2024.

S. Sharma and H. Babbar, "An analysis of Android malware and IoT attack detection with machine learning," *Journal of Cyber Security and Mobility*, vol. 12, no. 2, pp. 87–102, 2023.

J. Zhang, F. Zou, and J. Zhu, "Android malware detection based on deep learning," *IEEE communication on Information Forensics and Security*, vol. 14, no. 5, pp. 1120–1132, 2018.

R. Wang, J. Zheng, Z. Shi, and Y. Tan, "Detecting malware using graph embedding and DNN," *Neural Networks and Applications*, vol. 29, no. 15, pp. 233–245, 2025.

R. Pagán and K. Elleithy, "A multi-layered defense approach to safeguard against ransomware," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7545–7558, 2021.

F. Mercaldo, F. Martinelli, and A. Santone, "Fuzzy deep learning network for dynamic mobile malware detection," *Expert Systems with Applications*, vol. 203, no. 3, pp. 115005, 2023.

F. Mercaldo and A. Santone, "Image-based malware detection through a deep neuro-fuzzy model," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 202–214, 2023.

Rohith and G. Kaur, "A comprehensive study on malware detection and prevention techniques used by anti-virus," *Journal of Computer Security Research*, vol. 15, no. 3, pp. 121–137, 2021.

F. Mercaldo and A. Santone, "Formal equivalence checking for mobile malware detection and family classification," *IEEE Transactions on Software Engineering*, vol. 48, no. 6, pp. 1253–1264, 2022.