**International Journal of Advance and Innovative Research**
Volume 12, Issue 2 (XVII): April - June 2025
ISSN 2394 - 7780

# OPTIMIZING THREAT DETECTION IN CYBER SECURITY USING ML ALGORITHMS

**Rahul Brijlal Yadav**
Ramniranjan Jhunjhunwala college of Comm, Arts and Science

## ABSTRACT
*With the growing sophistication of cyber threats, the demand for timely and effective detection is greater than ever. The current research aims to identify and classify various types of cyber attacks using machine learning algorithms, specifically Naive Bayes, Quadratic Discriminant Analysis (QDA), and Multi-Layer Perceptron (MLP). We also examined attacks like Bots, DDoS attacks, and various Denial of Service variants like GoldenEye, Hulk, Slowhttptest, and Slowloris, and FTP-Patator, PortScan, and SSH-Patator. We chose the most suitable features for each attack type based on feature importance and trained the models accordingly. Our findings revealed that Naive Bayes performed incredibly well consistently, with high accuracy for all types of attacks. It was especially effective in identifying Bots, DDoS attacks, and various DoS attacks, with accuracy rates of over 90% in most cases. Although the MLP classifier displayed excellent performance in some attack types, its performance was highly sensitive to the type of attack. QDA, although helpful, tended to fall behind both Naive Bayes and MLP in accuracy. These results underscore the importance of selecting the most appropriate machine learning model for each type of threat. Naive Bayes proved to be a especially robust tool for real-time identification of threats and thus a valuable addition to the enhancement of cybersecurity strategies. This research underscores the importance of customized approaches in machine learning for cybersecurity and provides practical insights into the optimization of threat detection and response strategies.*

***Keywords:*** *Machine Learning, Threat Detection, Naive Bayes, Quadratic Discriminant Analysis, Multi-Layer Perceptron, Bot Detection, DDoS Attacks, DoS Attacks, Feature Importance, Attack Classification.*

## INTRODUCTION
With greater interdependence comes the growing risk of cyber-attacks on individuals, organizations, and social institutions. Those cyber-attacks that have exponentially increased with the widening digital networks and systems have dramatically increased in complexity and frequency of occurrence. Signature-based detection methods and static security protocols miserably fail to keep up with the evolving scenario. These conventional methods typically focus on established attack patterns and signatures and leave systems vulnerable to new and complex threats that do not conform to the established patterns.

Signature-based detection systems work by identifying certain patterns or signatures of known threats. Although very effective against known attacks, the signature-based approach has limited capability to deal with new or modified threats. For example, Advanced Persistent Threats are crafted to target particular systems over an extended period of time, usually evading detection through traditional methods because of their dynamic nature. Similarly, the advancement of malware and attack methodologies makes it challenging for the signature-based system to identify a new variation or sophisticated approach.

To these limitations, a massive shift has been realized towards the inclusion of AI and ML technologies into cybersecurity frameworks. AI and ML have a possibility of analyzing huge data volumes, uncovering hidden patterns, and identifying anomalies that might indicate malicious activities unlike traditional methods. Advanced techniques adapt to the dynamic nature of historical data and new information and can be used in predictive analyses with proactive and adaptive approaches in improving threat detection and prevention.

This research paper explores the use of different machine learning models in enhancing cybersecurity defenses. In this paper, we examine the performance of Naive Bayes, QDA, and MLP classifiers in distinguishing between different types of cyber-attacks and begin activities. The types of attacks looked at include bot attacks, DDoS attacks (Distributed Denial of Service), which involve many forms of DoS, including GoldenEye, Hulk, Slowhttptest, and Slowloris attacks, as well as FTP-Patator, PortScan, and SSH-Patator. These types of attacks were chosen because of their frequent occurrence and the wide effects both on individual persons and companies. Our study aims to find out how well these machine learning models can actually handle the weaknesses of the traditional approaches to cybersecurity. We have analyzed their ability in identifying and classifying such particular attack types and henceforth have compared the pros and cons of the approach over conventional techniques. Among them, DDoS attacks are most infamous for causing service disruption by flooding the network with traffic, whereas APTs and Slowloris-type DoS attacks are stealthy and persistent, which makes it difficult to detect and mitigate.

ISSN 2394 - 7780

The findings of this research are a contribution toward the deeper understanding of how machine learning can enhance cybersecurity measures, with insights into their practical applications and potential benefits. The paper is divided into several sections: we start with an overview of the current cybersecurity landscape and the limitations of traditional detection methods. Following this, we detail descriptions of the machine learning models applied in the paper. These include Naive Bayes, QDA, and MLP. Subsequent sections cover the experimental setup, results, and analysis for the above models. In conclusion, we discuss our implications regarding future cybersecurity practice and provide some directions to be considered in further research and development.

## LITERATURE REVIEW

The complexity of cyber threats, especially in the context of the Internet of Things (IoT), has led to the development of sophisticated models for threat detection. One such approach is the Mayfly Optimization with Regularized Extreme Learning Machine (MFO-RELM) model, which preprocesses IoT data to enhance threat classification accuracy. This model proves to have significant improvements for identifying cybersecurity threats in the IoT environment, indicating a need for advanced preprocessing techniques along with robust classification methods. More broadly, AI and ML are transforming the realm of cybersecurity, providing tools to better and more efficiently find threats. Traditional security measures are usually insufficient when combating highly sophisticated attacks, which makes AI and ML necessary. Various ML algorithms used for anomaly detection and malware classification have been reviewed to illustrate their effectiveness in real-world applications. This overview also addresses the challenges faced, including the need for large labelled datasets and the interpretability of ML models, and suggests future research directions such as explainable AI and unsupervised learning approaches. The other innovative approach, AI Sentry, combines machine learning and neural networks for enhancing real-time threat detection and prevention. The model shifts the paradigm of merely identifying known threats and also predicts zero-day attacks as well as unknown malicious activities. This system has a proven capability to allow AI to learn about new attack vectors and ensure high accuracy in threat detection than signature-based systems.

Application of deep learning techniques including multilayer perceptron and J48 has presented very promising results in terms of managing malicious traffic. To show how well these sophisticated approaches handle cybersecurity threats, they are being applied to datasets like Advanced Security Network Metrics & Non-Payload-Based Obfuscations ASNM-NPBO. Deep learning-based threat management demonstrates the necessity of implementing such cutting-edge strategies to control the steadily rising amount of hostile traffic. Even with the improvements, protecting against advanced persistent threats (APT) is still quite difficult. The investigation of artificial intelligence (AI) to increase detection rates is planned since traditional technologies frequently fail to identify these complex threats. Effective cybersecurity plans require striking a balance between the advantages of AI and the hazards involved. AI-powered autonomous threat hunting has become a major advancement in cybersecurity. Autonomous threat hunting integrates AI with traditional threat intelligence methodologies to improve the detection and response of security systems. It leverages various AI techniques, including machine learning models and natural language processing, for proactive identification and mitigation of threats.

Artificial intelligence is also integrated into AI-SIEM systems, which use artificial neural networks to make threat identification easier. This strategy focuses on using deep learning techniques to enhance detection performance and transforming security events into unique profiles. The efficiency of AI in network intrusion detection is demonstrated by the AI-SIEM system, which has been demonstrated to be more successful than traditional techniques. AI is important in cybersecurity for tasks like automated incident response and real-time threat identification. Large amounts of data can be analyzed by the AI system to spot any dangers and take the necessary precautions to lessen harm. This is the only method to guarantee strong protection of sensitive data and stay ahead of changing cyberthreats. The use of MLP was examined in the paper.

## METHODOLOGY

An important resource for network intrusion detection research is the canadian institute for cybersecurity's ids 2017 dataset. This dataset records network traffic in a controlled setting, encompassing both benign and malevolent activity. Along with innocuous traffic, it encompasses a variety of attack types, including dos, ddos, and other prevalent vectors. Numerous attributes in the dataset, such as flow time, packet length, and protocol kinds, define the properties of network packets. When developing and evaluating machine learning models for intrusion detection and classification, each of these characteristics is essential. One of the most popular datasets in academic and industrial settings for creating and improving algorithms to raise the degree of cybersecurity is the ids 2017 dataset.

ISSN 2394 - 7780

Our methodical approach to data preprocessing ensures quality and consistency by preparing the material for analysis. First, we address missing data by replacing infinite values with NaN and removing rows with missing "Flow Duration" values. The dataset is then cleaned by removing any residual NaN values. Numerical columns are cleaned and then normalized using conventional scale. Fair comparison and analysis are made possible by ensuring that every feature has a zero mean and unit variance. Label encoding is used to convert all other categorical columns to numeric values, with the exception of the target variable "Label." The value -1 is used to handle anomalies in special instances, such as 'Infinity'. Following the cleaning of each data set individually, the cleaned data frame will be concatenated into the cleaned Data Frame into a single comprehensive data frame that will be saved onto a new CSV file for other further analysis. This process ensures uniform cleaning, normalization and encoding of the data across the field.

An essential first step in comprehending and improving the effectiveness of machine learning models in identifying network threats is feature importance analysis. We evaluate the relative significance of several variables for differentiating between attack types and benign activities using the Random Forest algorithm. The features that have the biggest effects on classification accuracy are determined by this analysis. The knowledge acquired from this procedure is crucial for improving machine learning models since it enables us to rank important features and exclude less important ones, increasing the efficacy and efficiency of the models. Furthermore, knowing the significance of features enhances model interpretability, clarifies the foundation for predictions, and facilitates the creation of threat detection systems that are more accurate and dependable. Using this technique helps to maximize model performance and guarantee that the most pertinent data attributes are used in network attack classification.

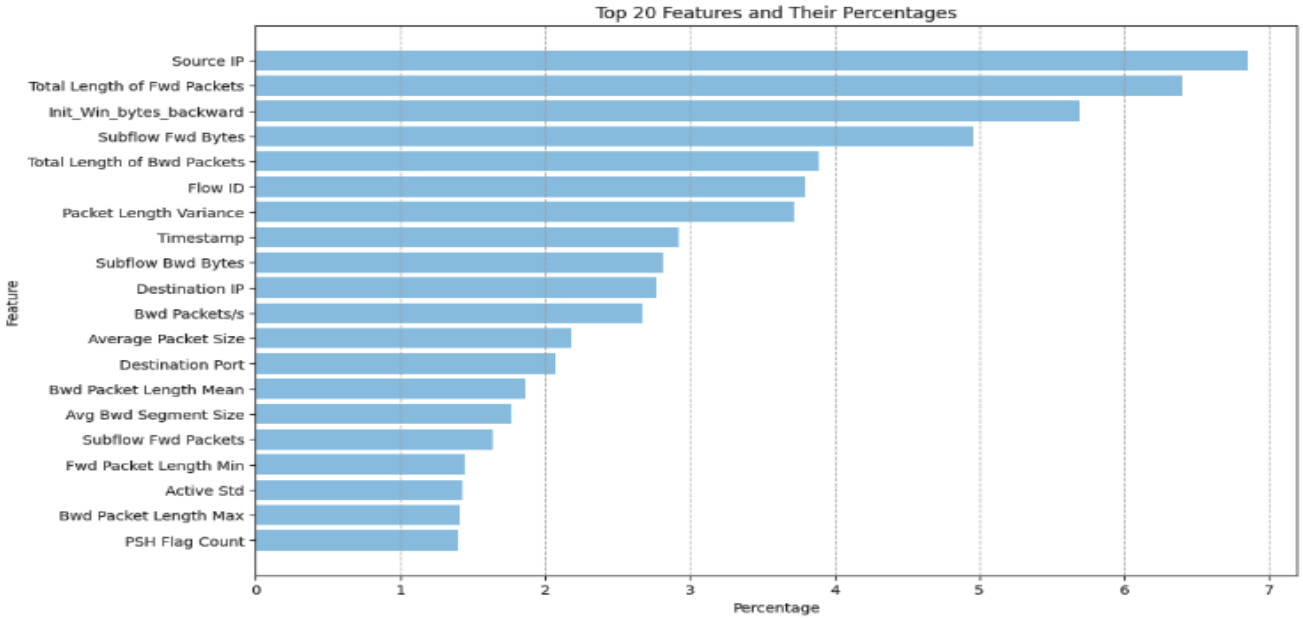


***Figure 1*** Feature Selection

ISSN 2394 - 7780

We evaluated several machine learning models to classify various kinds of network attacks comprehensively. In this regard, we utilized Naive Bayes, Quadratic Discriminant Analysis (QDA), and Multi-Layer Perceptron (MLP) classifiers. Each model had been chosen based on distinct approaches towards classification and handling multiple data characteristics.

Naive Bayes was chosen for preliminary classification jobs because of its ease of use and effectiveness when working with huge datasets that contain categorical features. QDA was chosen because it can more flexibly simulate decision boundaries between classes by taking feature covariance into consideration. MLP was added because, because to its neural network architecture, it can efficiently handle non-linear correlations in the data and capture intricate patterns. An input layer, hidden layers, and an output layer make up the MLP classifier's several layers. The hidden layers usually have non-linear activation functions. By adding non-linearity to the model using activation functions like ReLU or sigmoid functions in the hidden layers, MLP is able to capture complex patterns and correlations. MLP trains by optimizing the loss function by using back-propagation to adjust its weights to model complex, nonlinear interactions between features.

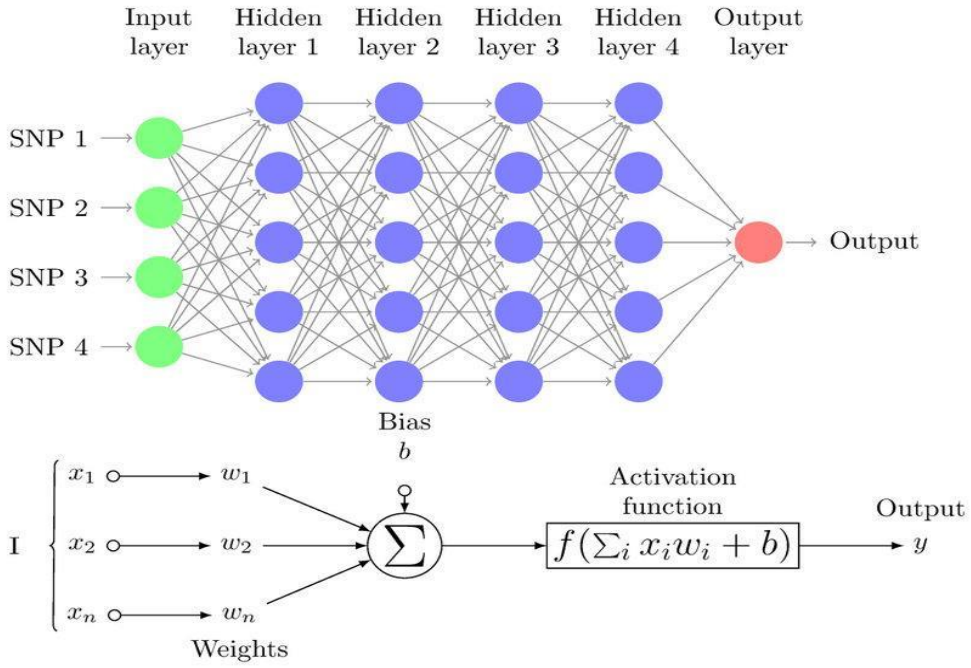


***Figure 2*** Multilayer perceptron

Figure 2 depicts the architecture of the Multilayer Perceptron. Models were trained on datasets customized for each attack type using preselected features that are significant for classification. Subsequently, rigorous testing was conducted to evaluate the performance of each model. Based on the comparison of accuracy metrics across different attack types, we sought to determine which model offers the best classification performance, thereby providing insights into their practical applicability for network intrusion detection. This evaluation is important as it helps in understanding the strengths and limitations of each model, guiding the selection of appropriate techniques for enhancing network security systems. The results provide valuable benchmarks for deploying machine learning-based intrusion detection systems and contribute to advancing the field of cybersecurity.

**RESULTS**

This study evaluates the performance of three machine learning models, Naive Bayes, Quadratic Discriminant Analysis (QDA), and Multi-Layer Perceptron (MLP), in classifying different types of network attacks. The results show important variations in model accuracy based on attack type.

Naive Bayes provided good performance, especially for detection of Bot attacks and SSH-Patator with 96.72% and 100% respectively. It also gave pretty good accuracy for FTP-Patator with 99.95% and PortScan with 99.99%. Nonetheless, its performance declined significantly for some DoS attacks. For example, Naive Bayes provided poor performance for DoS GoldenEye with an accuracy of 99.17% and only 99.51% against DoS Hulk. As for QDA, it is underperforming in nearly all attack types. Its accuracy was very low for different DoS attacks that were between 32.28% and 33.36%. The best accuracy for QDA was at SSH-Patator with 33.56%, but on average, the model performed poorly in classification. MLP was the best model with an accuracy of 99.96% for Bot attacks, 97.42% for FTP-Patator, and 98.46% for PortScan. Despite its generally high accuracy,

ISSN 2394 - 7780

MLP showed lower performance for certain attacks, including DDoS and DoS slowloris with accuracies of 71.89% and 35.45%, respectively.

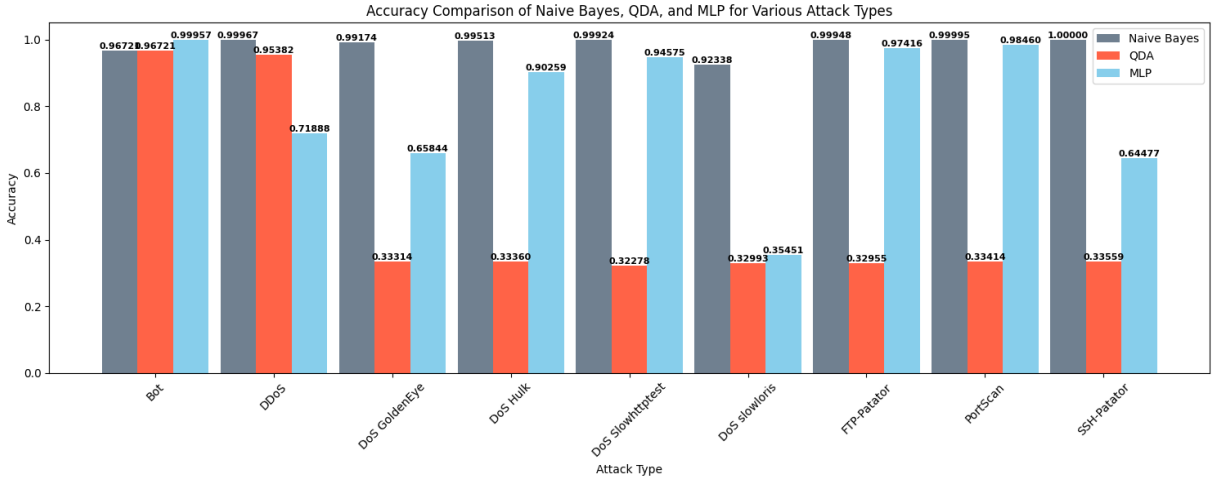


***Figure 3*** Accuracy comparison of Naive Bayes, QDA, and MLP for different network attacks.

As given in Figure2 below, the bar graph provides a visual comparison between the accuracy of the various models and attack types. This diagram shows that overall, MLP is relatively very effective in achieving higher accuracies when compared to QDA which, generally, performs poorly. Naive Bayes is also performing well, and specifically for the detection of some attack types, it has good performance, although not outperforming MLP constantly. The results show that different models are effective in various attacks, and the accuracy of MLP on most attacks reveals the possibility of using such models in cybersecurity to improve the network intrusion detection system. However, the lower performance of QDA across most attack types brings forth the point that alternative or hybrid models would be needed to improve overall detection capabilities.

## CONCLUSION

It highlights the capacity of complex algorithms in enriching network defense mechanisms for cybersecurity attacks. The effectiveness of MLP clearly shows the potential it holds in giving accurate results on a broad range of attacks, placing it firmly at the forefront for real-time identification and mitigating threat conditions. Its robustness and ability to deliver high accuracy in most scenarios makes it a suitable candidate for incorporation into comprehensive cybersecurity frameworks. Challenges identified with QDA point towards the inability of traditional statistical models to cope up with complex and diverse attack patterns. This means that QDA alone may not be enough for strong network security, and more advanced or hybrid approaches are required that take advantage of the strengths of multiple models. In addition, although Naive Bayes performed well in many attack types, the results show that no single model is a panacea. This variability in accuracy across different attacks suggests that a multifaceted approach, combining different models, may offer a more balanced and effective defense strategy.

Future work should be on fine-tuning the MLP model and exploring ensemble methods that combine the strengths of this model with other models. Further, exploring the reasons for the poor performance of some models can help in understanding their limitations and guiding improvements. As the cyber threat landscape continues to evolve, adaptive and intelligent machine learning solutions will be necessary to stay ahead of emerging attack vectors and enhance overall network security.

## REFERENCE

[1] J. Li, “Cyber security meets artificial intelligence: a survey,” *Frontiers Inf Technol Electronic Eng*, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: 10.1631/FITEE.1800573.

[2] F. Alrowais, S. Althahabi, S. S. Alotaibi, A. Mohamed, M. Ahmed Hamza, and R. Marzouk, “Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment,” *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 687–700, 2023, doi: 10.32604/csse.2023.030188.

[3] Dr. N. Katiyar, Mr. S. Tripathi, Mr. P. Kumar, Mr. S. Verma, Dr. A. K. Sahu, and Dr. S. Saxena, “AI and Cyber-Security: Enhancing threat detection and response with machine learning.,” *eatp*, Apr. 2024, doi: 10.53555/kuey.v30i4.2377.

ISSN 2394 - 7780

[4] S. Rangaraju, "AI SENTRY: REINVENTING CYBERSECURITY THROUGH INTELLIGENT THREAT DETECTION," *EPHIJSE*, vol. 9, no. 3, pp. 30–35, Dec. 2023, doi: 10.53555/ephijse.v9i3.211.

[5] T. T. Teoh, G. Chiew, E. J. Franco, P. C. Ng, M. P. Benjamin, and Y. J. Goh, "Anomaly detection in cyber security attacks on networks using MLP deep learning," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Shah Alam: IEEE, Jul. 2018, pp. 1–5. doi: 10.1109/ICSCEE.2018.8538395.

[6] K. Hasan, S. Shetty, and S. Ullah, "Artificial Intelligence Empowered Cyber Threat Detection and Protection for Power Utilities," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, Los Angeles, CA, USA: IEEE, Dec. 2019, pp. 354–359. doi: 10.1109/CIC48465.2019.00049.

[7] S. R. Sindiramutty, "Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence".

[8] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," *IEEE Access*, vol. 7, pp. 165607–165626, 2019, doi: 10.1109/ACCESS.2019.2953095.

[9] M. Rizvi, "Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention," *IJAERS*, vol. 10, no. 5, pp. 055–060, 2023, doi: 10.22161/ijaers.105.8.

[10] L. Van Efferen and A. M. T. Ali-Eldin, "A multi-layer perceptron approach for flow-based anomaly detection," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, Marrakech, Morocco: IEEE, May 2017, pp. 1–6. doi: 10.1109/ISNCC.2017.8072036.

[11] B. R. Maddireddy and B. R. Maddireddy, "Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment," vol. 01, no. 02, 2020.

[12] A. R. P. Reddy, "THE ROLE OF ARTIFICIAL INTELLIGENCE IN PROACTIVE CYBER THREAT DETECTION IN CLOUD ENVIRONMENTS," vol. 19, no. 12, 2021.