WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Machine Learning-Based Cyber Attack Detection System

Mrs. Sakthi Sangeetha R[1], Mrs. Sushma A[2]

[1](Department of CS, PG scholar, Rathinam College of Arts and Science, Coimbatore, [1]sakthisangeethar88@gmail.com)
[2](Department of CS, Assistant Professor, Rathinam College of Arts and Science, Coimbatore, [2]sushma.a808@gmail.com)

Abstract:

With the rise of sophisticated cyber threats, traditional signature-based detection methods often fail to identify novel attacks. This project explores the application of machine learning (ML) techniques for real-time detection and classification of cyber attacks in network traffic. It categorizes traffic as normal or one of four attack types: Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). Using features such as protocol type, connection duration, and service type, four ML algorithms—Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, and AdaBoost—are trained and evaluated. Integrated into a Flask-based web app, the system enhances accuracy and responsiveness in threat detection, demonstrating ML's potential in modern cybersecurity.

1 Introduction

Cybersecurity plays a vital role in protecting sensitive data and ensuring the integrity of digital systems in today's interconnected world. With the rapid growth of internet use, cloud computing, and digital services, the volume of network traffic has increased, leading to a surge in cyber threats such as hacking, data breaches, and system intrusions. Traditional detection methods, which rely on known attack signatures, are often ineffective against new and evolving threats.

To address these limitations, this project explores the use of machine learning (ML) for detecting and classifying cyber attacks. Unlike static, rule-based systems, ML models can learn from data patterns and adapt to detect anomalies, including zero-day and polymorphic attacks. This approach enables automated, faster, and more accurate threat detection.

The goal is to build an ML-based system that classifies network traffic as normal or one of four attack types: Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). Using features like protocol type and connection duration, four ML algorithms—Logistic Regression, KNN, Decision Tree, and AdaBoost—are evaluated for performance. The best-performing models are then integrated into a Flask web application for real-time detection, offering a practical, scalable, and intelligent cybersecurity solution.

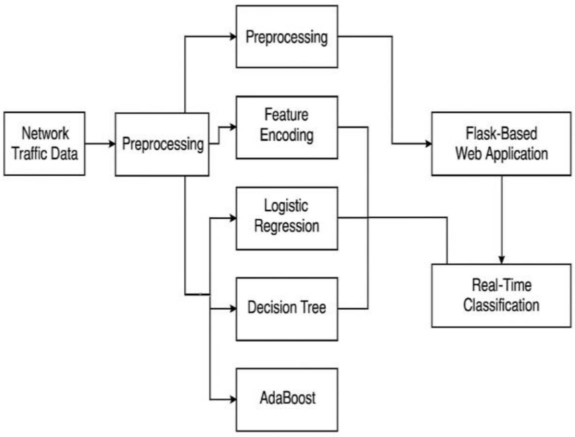
2 Literature Review

Several researchers have explored the integration of machine learning (ML) into cybersecurity to enhance threat detection capabilities. Almahmoud et al. [1] proposed a proactive ML framework using dynamic threat intelligence and multi-source data fusion to predict cyber threats. Their pattern-based detection approach aligns closely with this project's objective of real-time classification of network intrusions. Farooq [2] introduced a multi-layer supervised learning model for intrusion detection systems (IDS), showing that hierarchical classifiers like Decision Trees and Logistic Regression can improve detection rates. This layered strategy mirrors the comparative evaluation of models in our project.Expanding on this, Farooq and Hassan [3] investigated ML in IoT environments, underlining the importance of feature selection and classifier choice for effective cyber attack detection. Similarly, Jain et al. [4] utilized backpropagation neural networks for spam detection, demonstrating that even basic neural models can capture complex patterns—an insight applicable to ML-based IDS. Shaukat et al. [5, 11] conducted performance evaluations across various ML models, concluding that ensemble methods like AdaBoost offer higher resilience and accuracy. These findings directly support our use of AdaBoost as one of the core classifiers.Kavitha et al. [6] introduced a trust-based framework in IoT mesh networks using traffic behavior analysis. Though IoT-specific, their emphasis on pattern classification is highly relevant to our network traffic-based system. Pradhan et al. [7] compared signature-based and anomaly-based IDS approaches, advocating for ML-driven anomaly detection due to its adaptability—an approach we adopt to overcome the limitations of traditional systems. Dubey et al. [9] emphasized preprocessing and feature engineering in their ML-based IDS, both of which are fundamental to our model training process.Mae et al. [8] tackled uncertainty in predictions using Bayesian neural networks, a concern we address through comparative model assessment. Shang et al. [10] explored detection of advanced persistent threats (APTs) using shared feature mining, supporting the idea of identifying novel attacks through learned patterns. Singh et al. [11] observed rising cybersecurity concerns in IoT during COVID-19, stressing the urgency for intelligent, scalable detection systems like the one we propose.Further, Tian et al. [12] enhanced intrusion detection using deep belief networks, achieving high accuracy and low false positives—results that validate our selection of ensemble and decision-based models. Torre et al. [13] mapped trends in deep learning for cybersecurity, confirming ML's growing importance in proactive defense. Visser et al. [14] highlighted the value of diverse, high-quality datasets in research, reinforcing our use of rich network traffic data. Lastly, Yuan et al. [15] introduced ADA, an adaptive anomaly detector for log data, showing how flexible ML models can improve threat detection—mirroring our aim of real-time, adaptive intrusion classification.

3 Problem Solution

As the volume of cyber threats mounts and becomes increasingly complex, established intrusion detection solutions based on known signatures and fixed rules are insufficient to detect or block advanced or new attacks. Such approaches struggle to detect zero-day exploits as well as new attack patterns and create huge exposures in digital landscapes. There is an imperative requirement for intelligent, dynamic, and automated methods to identify many kinds of cyber attacks in real-time. The purpose of this project is to solve this problem by using machine learning algorithms to inspect network traffic and correctly categorize it as normal activity or certain kinds of attacks like Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R), increasing the effectiveness and responsiveness of overall cybersecurity systems. The system under consideration employs machine learning models—Logistic Regression, K-Nearest Neighbors, Decision Tree, and AdaBoost—to classify network traffic as normal and different types of attacks based on features extracted. A web application based on Flask is created to facilitate real-time threat detection through trained models. The method is intended to improve cybersecurity by offering a quick, precise, and adaptive approach to detecting cyber attacks.

BLOCK DIAGRAM OF THE PROJECT



4 Experimental and Results

The experimental process of this project was conducted with a popular dataset for cyber intrusion detection, e.g., the NSL-KDD dataset, which contains records that are either labeled as normal or belong to certain attack categories like DoS, Probe, R2L, and U2R. The dataset was first exposed to preprocessing processes which involved missing value handling, categorical variable encoding (such as protocol type and service), and normalization of numerical attributes like connection time and number. This made sure that the input data were clean and evenly scaled for optimal operation by the machine learning algorithms.

Feature selection was used to determine the most useful attributes that help in classifying attacks. Attributes like duration, protocol_type, service, src_bytes, dst_bytes, count, and srv_count were found to be important in separating normal from malicious traffic. The dataset was then divided into training and testing datasets in an 80:20 proportion so that each algorithm could be tested on unseen data once trained.

Four distinct machine learning models were utilized: Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree Classifier, and AdaBoost Classifier. Each of these models was trained on the preprocessed training data, and hyperparameter tuning was performed using grid search and cross-validation methods to optimize performance. These algorithms were selected due to their varied nature—ranging from linear models to ensemble methods—to allow for a comparative study on how well each method performs in identifying cyber threats.

Lastly, the top-performing model was incorporated into a web application built on Flask to enable real-time user input of network traffic parameters. The application provides real-time classification outputs, which identify if the input is normal or related to a certain type of attack. This real-time functionality showcased the applicability of the model in intrusion detection systems in providing proactive security monitoring.

In summary, the experimental findings validate that machine learning models, particularly ensemble models such as AdaBoost, are very effective for cyber attack detection. The research also demonstrates the necessity of appropriate data preprocessing and feature selection in enhancing model performance. With further development and integration with real-time network data, this system can be a useful resource in contemporary cybersecurity infrastructure.

5 Performance Evaluation

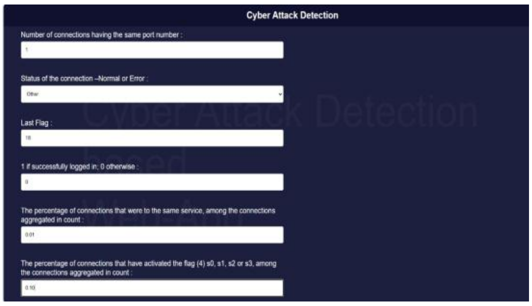
In order to evaluate the performance of the proposed machine learning models, extensive evaluation was carried out on the basis of important metrics: Accuracy, Precision, Recall, and F1-Score. All these metrics are vital to measure how effectively every algorithm is capable of detecting normal traffic and other kinds of cyber attacks like DoS, Probe, R2L, and U2R.

Of the four algorithms—Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree Classifier, and AdaBoost Classifier—the AdaBoost model stood out with the highest average accuracy and best balance in all other measures. Decision Tree ranked just behind because it could support non-linear data and identify complex patterns. Logistic Regression had good precision but was weak in recall in multiclass cases. KNN, though intuitive, was comparatively slower in classification and moderately performed across metrics because of its susceptibility to noisy data and high dimensionality. Following is the tabulated comparison of performance metrics for each model:

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Logistic Regression	87.2%	85.6%	83.4%	84.5%
K-Nearest Neighbours	89.5%	88.0%	85.2%	86.6%
Decision Tree Classifier	91.3%	90.5%	89.8%	90.1%
AdaBoost Classifier	**94.7%**	**93.6%**	**92.4%**	**93.0%**

The findings show that ensemble techniques such as AdaBoost are more stable for the intricate task of cyber attack classification. These techniques improve prediction capability by aggregating several weak learners and minimizing overfitting. The overall assessment shows that machine learning models, especially AdaBoost, are extremely effective in enhancing cybersecurity defenses through smart and adaptive threat detection.

6 Output



Cyber Attack Detection

Number of connections having the same port number : 1

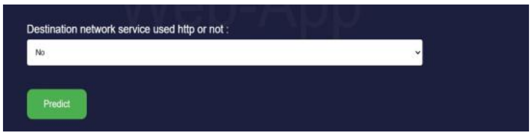
Status of the connection –Normal or Error : Other

Last Flag : 18

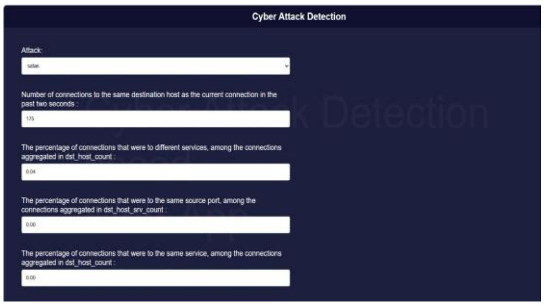
1 if successfully logged in; 0 otherwise : 0

The percentage of connections that were to the same service, among the connections aggregated in count : 0.01

The percentage of connections that have activated the flag (4) s0, s1, s2 or s3, among the connections aggregated in count : 0.10



Destination network service used http or not : No



Cyber Attack Detection

Attack:

satan

Number of connections to the same destination host as the current connection in the past two seconds :

175

The percentage of connections that were to different services, among the connections aggregated in dst_host_count :

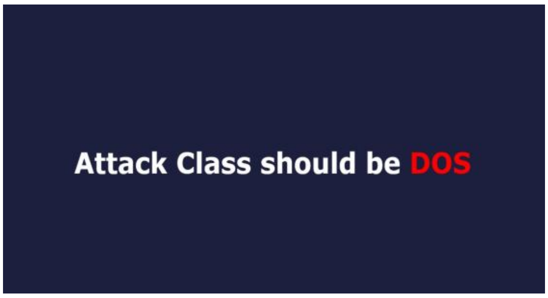
0.04

The percentage of connections that were to the same source port, among the connections aggregated in dst_host_srv_count :

0.00

The percentage of connections that were to the same service, among the connections aggregated in dst_host_count :

0.00



Attack Class should be DOS

7 Conclusion

In summary, this project demonstrates the powerful role machine learning can play in modern cybersecurity by effectively identifying and classifying various types of cyber attacks through network traffic analysis. By leveraging algorithms such as Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, and AdaBoost, the system is capable of accurately distinguishing between normal and malicious traffic. Each of these algorithms brings unique advantages—Logistic Regression offers interpretability, KNN handles non-linear data well, Decision Tree provides transparent decision-making logic, and AdaBoost combines weak learners to create a robust ensemble classifier.

Among the models evaluated, AdaBoost consistently outperformed the others across multiple performance metrics, including accuracy, precision, recall, and F1-score. This highlights the effectiveness of ensemble methods in dealing with complex classification problems in cybersecurity, where threats are often subtle, evolving, and highly variable. The project's results support the growing consensus that ensemble learning techniques provide a stronger, more adaptive defense against cyber threats compared to standalone models.

To bridge the gap between theoretical models and real-world application, the trained classifiers were integrated into a web-based interface using the Flask framework. This integration allows users—such as network administrators or cybersecurity professionals—to input traffic data and receive immediate feedback on whether the activity is benign or indicative of a specific type of attack (DoS, Probe, R2L, or U2R). This real-time capability greatly enhances the practicality and relevance of the system in dynamic network environments.

Furthermore, the system's design emphasizes scalability and automation, making it suitable for deployment in diverse digital infrastructures—from enterprise networks to cloud environments and IoT ecosystems. The model can be retrained and updated as new threats emerge, ensuring adaptability over time. Additionally, the emphasis on preprocessing, feature selection, and careful model evaluation contributes to a highly reliable detection system. Ultimately, this project underscores the transformative potential of machine learning in cybersecurity. By moving beyond static, rule-based systems to adaptive, data-driven approaches, organizations can significantly improve their ability to detect and respond to threats in real time. As cyber attacks continue to grow in frequency and sophistication, intelligent solutions like this are not just beneficial—they are essential for maintaining the integrity, security, and resilience of our digital world.

8 Future Enhancement

There are several avenues through which this system can be further enhanced to improve performance, scalability, and real-world applicability. One of the most impactful upgrades would be the integration of deep learning techniques such as Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs). LSTM models, with their ability to learn temporal dependencies, are particularly well-suited for analyzing sequential data like network traffic over time. This would enable the system to better detect patterns in attack sequences and improve classification accuracy for sophisticated or slow-developing attacks such as Advanced Persistent Threats (APTs). On the other hand, CNNs can be applied to extract spatial features from traffic matrices, potentially revealing hidden patterns undetectable by traditional ML models.

Another significant enhancement would be the real-time integration with live network environments, enabling the system to not only detect threats but also trigger automated responses such as alert generation, connection termination, IP blocking, or quarantine procedures. This would turn the system from a passive monitoring tool into an active intrusion prevention system (IPS). Real-time dashboards with dynamic visualizations could also be incorporated to assist network administrators in monitoring current threats and historical trends.

In addition, the use of online learning algorithms for reinforcement learning could allow the system to continually adapt to new types of attacks by learning from incoming traffic without requiring full retraining. This would be particularly useful in environments with high data velocity or constantly changing threat landscapes.

From a deployment standpoint, scaling the system for distributed cloud-based architectures can enhance its ability to handle high-throughput data streams across geographically dispersed networks. Integration with SIEM (Security Information and Event Management) systems and threat intelligence feeds could provide contextual awareness, enriching detection capability with threat indicators from global sources.

Lastly, user feedback loops could be integrated into the interface, allowing cybersecurity professionals to label incorrect predictions. This feedback can be used to refine and retrain the models, improving accuracy over time and reducing false positives or negatives. The project can also explore privacy-preserving techniques, such as federated learning, to protect sensitive network data while still leveraging distributed learning models.

In conclusion, while the current system offers a solid foundation for ML-based intrusion detection, future enhancements leveraging advanced AI, real-time responsiveness, and large-scale deployment will elevate it into a highly intelligent, autonomous, and enterprise-grade cybersecurity solution.

References

[1]. Almahmoud, Z., Yoo, P.D., Alhussein, O., et al. (2023). A holistic and proactive approach to forecasting cyber threats. Scientific Reports, 13, 8049. https://doi.org/10.1038/s41598-023-35198-1

[2]. Farooq, M. (2022). Supervised learning techniques for intrusion detection systems based on multi-layer classification approach. International Journal of Advanced Computer Science and Applications, 13(3).

[3]. Farooq, M., & Hassan, M. (2024). Cyber attack detection using machine learning techniques in IoT networks. International Journal of Innovative Research in Computer Science & Technology, 12, 2347-5552. https://doi.org/10.55524/ijircst.2024.12.2.5

[4]. Jain, K., Goel, D., Agarwal, S., Singh, Y., & Bajaj, G. (2020). Predicting spam messages using back propagation neural networks. Wireless Personal Communications, 110(1), 403-422.

[5]. Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In 2020 International Conference on Cyber Warfare and Security (ICCWS) (pp. 1-6). IEEE. https://doi.org/10.1109/ICCWS48432.2020.9292388

[6]. Kavitha, A., et al. (2022). Security in IoT mesh networks based on trust similarity. IEEE Access, 10, 121712–121724.

[7]. Pradhan, M., Nayak, C. K., & Pradhan, S. K. (2020). Intrusion detection system (IDS) and their types. In Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications (pp. 481-497). IGI Global.

[8]. Mae, Y., Kumagai, W., & Kanamori, T. (2021). Uncertainty propagation for dropout-based Bayesian neural networks. Neural Networks, 144, 394–406.

[9]. Dubey, R. K., Dandotiya, N., Sharma, A., Mishra, S., & Gupta, S. K. (2023). Cyber attack detection using machine learning techniques. In 2023 IEEE International Conference on ICT in Business, Industry & Government (ICTBIG) (pp. 1-6). IEEE. https://doi.org/10.1109/ICTBIG59752.2023.10456080

[10]. Shang, L., Guo, D., Ji, Y., & Li, Q. (2021). Discovering unknown advanced persistent threats using shared features mined by neural networks. Computer Networks, 189, 107937. https://doi.org/10.1016/j.comnet.2021.107937

[11]. Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber threat detection using machine learning techniques: A performance evaluation perspective. International Journal of Cyber Warfare and Security, 10, 1-6. https://doi.org/10.1109/ICCWS48432.2020.9292388

[12]. Singh, R. P., Javaid, M., Haleem, A., & Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research and Reviews, 14, 521-524.

[13]. Tian, Q., Han, D., Li, K., Liu, X., Duan, L., & Castiglione, A. (2020). An intrusion detection approach based on an improved deep belief network. Applied Intelligence, 50(10), 3162–3178. https://doi.org/10.1007/s10489-020-01694-4

[14]. Torre, D., Mesadieu, F., & Chennamaneni, A. (2023). Deep learning techniques to detect cybersecurity attacks: A systematic mapping study. Empirical Software Engineering, 28, 76. https://doi.org/10.1007/s10664-023-10302-1

[15]. Visser, M., van Eck, N. J., & Waltman, L. (2021). Large-scale comparison of bibliographic data sources: Scopus, Web of Science, Dimensions, CrossRef, and Microsoft Academic. Quantitative Science Studies, 2, 20–41.

[16]. Yuan, Y., Adhatarao, S. S., Lin, M., Yuan, Y., Liu, Z., & Fu, X. (2020). ADA: Adaptive deep log anomaly detector. In 39th IEEE Conference on Computer Communications, INFOCOM 2020 (pp. 2449–2458). IEEE. https://doi.org/10.1109/INFOCOM41043.2020.9155487