

A ROBUST MACHINE LEARNING ENSEMBLE FOR INTRUSION DETECTION USING MAJORITY VOTING

¹ Mrs. E. Pavithra, ² B. Rakesh Naik, ³ B. Bhuvana Terisha, ⁴ B. Madhuri Priya, ⁵ CH. Sai Ram

¹ Assistant Professor in Department of CSE Sri Indu College of Engineering & Technology -Hyderabad.
^{2,3,4,5} UG Scholars in Department of CSE Sri Indu College of Engineering & Technology-Hyderabad.

Abstract

The rapid expansion of internet services and network-driven applications has led to a substantial rise in cyberattacks and security threats. Intrusion Detection Systems (IDS) are essential for monitoring network activity and identifying unauthorized access, malicious behavior, and potential vulnerabilities. However, conventional IDS solutions often struggle with high false alarm rates and reduced accuracy when processing large and complex network traffic. To overcome these limitations, this study presents a machine learning-based Intrusion Detection System that employs an incremental majority voting strategy. The proposed framework integrates multiple classifiers and combines their predictions through a majority voting mechanism to enhance detection reliability. By incorporating incremental learning, the system continuously updates its knowledge with newly available data, enabling it to adapt to emerging and evolving cyber threats. Experimental results show that the proposed approach improves overall detection accuracy while minimizing false positives. The system effectively detects a variety of attack categories, including DoS, Probe, R2L, and U2R. Comparative analysis confirms that the incremental majority voting model outperforms individual machine learning classifiers, making it a practical and efficient solution for strengthening modern network security.

Keywords

Intrusion Detection System, Machine Learning, Cyber Security, Network Security, Majority Voting, Incremental Learning, Classification Algorithms.

I. INTRODUCTION

The rapid development of computer networks and internet technologies has significantly transformed modern communication systems. Organizations, industries, and individuals increasingly rely on network infrastructures for

information exchange, cloud computing, and digital service delivery. However, this rapid growth has also increased the exposure of network systems to various cybersecurity threats such as hacking, malware infections, denial-of-service attacks, phishing, and unauthorized data access. These cyber threats can result in severe

financial losses, compromise sensitive information, and disrupt critical organizational operations. Consequently, ensuring network security has become one of the most important challenges in modern information technology environments [1].

To protect network infrastructures from such malicious activities, Intrusion Detection Systems (IDS) have become an essential component of modern cybersecurity frameworks. IDS are designed to monitor network traffic and system activities in order to detect suspicious behavior and potential security violations. Traditional IDS techniques mainly rely on signature-based detection methods, where predefined attack signatures are used to identify known threats. Although these systems are effective in detecting previously known attacks, they are often unable to detect new or unknown attack patterns, commonly referred to as zero-day attacks [2].

In recent years, machine learning techniques have gained significant attention in intrusion detection research due to their ability to analyze large-scale network data and automatically learn complex attack patterns. Machine learning-based IDS models can classify network traffic into normal and malicious categories by learning from historical datasets. These intelligent systems provide improved detection capabilities compared to traditional rule-based systems, as they can detect unknown attacks by analyzing patterns and anomalies in network traffic data [3].

Several machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), Random Forests, Naïve Bayes, and Neural Networks have been successfully applied for intrusion detection tasks. These models analyze various network features such as packet size, protocol type, connection duration, and traffic frequency to identify abnormal behaviors. However, relying on a single machine learning model may not always provide optimal detection performance due to variations in dataset characteristics, attack complexity, and model limitations [4].

To address this limitation, ensemble learning techniques have been introduced in intrusion detection systems. Ensemble learning combines multiple classifiers to improve prediction performance and reduce model bias. Among these techniques, majority voting is one of the most commonly used ensemble methods where multiple classifiers independently analyze input data and the final decision is determined based on the majority prediction of the classifiers. This approach enhances classification robustness and improves detection accuracy [5].

In addition to ensemble learning, incremental learning has emerged as an effective approach for handling dynamic network environments. Incremental learning allows machine learning models to continuously update their knowledge using newly available data without retraining the entire model from scratch. This capability is particularly important in cybersecurity

applications where new attack patterns constantly evolve and require continuous system adaptation [6].

Therefore, integrating incremental learning with ensemble techniques such as majority voting can significantly improve the efficiency and adaptability of intrusion detection systems. The proposed research focuses on developing an Incremental Majority Voting Intrusion Detection System that combines multiple machine learning classifiers with an incremental learning mechanism to enhance detection accuracy, reduce false alarm rates, and improve the system's ability to detect emerging cyber threats in dynamic network environments.

II. LITERATURE SURVEY

Intrusion detection has been an important research area in network security for several decades. Researchers have proposed numerous techniques including statistical analysis, rule-based detection, data mining methods, and machine learning approaches to identify malicious network activities. With the increasing complexity of cyber-attacks, traditional intrusion detection techniques have gradually evolved into intelligent systems that utilize artificial intelligence and data-driven approaches to enhance network security and improve detection efficiency [1]. One of the earliest contributions to intrusion detection research was made by Denning, who introduced an anomaly detection model that monitored system activities and

detected deviations from normal behavior patterns. This model laid the foundation for many modern anomaly-based intrusion detection systems by demonstrating that abnormal activities could be identified through behavioral analysis and statistical profiling of system activities [2]. Lee and Stolfo later introduced a data mining-based intrusion detection framework that utilized machine learning techniques to analyze audit data and detect network intrusions. Their research demonstrated that classification algorithms could effectively identify patterns associated with malicious activities in network traffic data and significantly improve intrusion detection capabilities [3]. Mukkamala et al. conducted a comparative study on different machine learning algorithms including neural networks and support vector machines for intrusion detection. Their findings indicated that machine learning models could significantly improve intrusion detection accuracy compared to traditional rule-based systems. The study also emphasized the importance of feature selection in improving the overall performance and efficiency of IDS models [4]. Tsai et al. presented a comprehensive survey of machine learning techniques applied to intrusion detection systems. Their work analyzed various supervised and unsupervised learning methods including clustering, classification, and hybrid models for identifying network attacks. The survey concluded that machine learning-based IDS can effectively detect both known and unknown attack patterns when trained with appropriate

datasets and feature engineering methods [5]. Sommer and Paxson investigated the practical challenges of applying machine learning in intrusion detection systems. Their research highlighted the importance of high-quality datasets, efficient feature extraction methods, and realistic evaluation procedures. They also emphasized that machine learning models must be carefully designed to handle noisy network data and high-dimensional features commonly present in real-world network traffic environments [6]. In recent years, researchers have explored ensemble learning techniques to improve the performance of intrusion detection systems. Ensemble models combine predictions from multiple classifiers to enhance classification accuracy and robustness. Majority voting is a widely used ensemble strategy where each classifier contributes a vote for the predicted class, and the final decision is determined based on the majority vote among all classifiers [7]. Incremental learning approaches have also gained attention for their ability to handle continuously evolving network environments. These models allow intrusion detection systems to update their knowledge dynamically as new network traffic data becomes available. Incremental learning reduces the need for retraining models from scratch and improves scalability in real-time monitoring systems [8]. Despite these advancements, several challenges still remain in the development of effective intrusion detection systems. Issues such as high false alarm rates, difficulty in detecting

zero-day attacks, computational complexity, and the requirement of large labeled datasets continue to limit IDS performance. Therefore, integrating ensemble learning with incremental learning strategies has emerged as a promising research direction for improving the efficiency and adaptability of modern intrusion detection systems [9].

III. EXISTING SYSTEM

Traditional intrusion detection systems (IDS) have been widely used to protect computer networks from unauthorized access and malicious activities. These systems mainly rely on **signature-based detection techniques**, where a database of previously identified attack patterns is maintained. Incoming network traffic is continuously monitored and compared against these stored signatures to determine whether the traffic corresponds to a known attack. Signature-based IDS such as Snort and Suricata have been widely adopted because they provide high accuracy when detecting attacks that already exist in the signature database. However, the major limitation of this approach is its inability to detect **new or unknown attacks**, also known as zero-day attacks. Since these attacks do not have predefined signatures, traditional systems fail to recognize them.

Another widely used approach is **anomaly-based intrusion detection**, which identifies deviations from normal network behavior. In this method, a baseline model of normal network activity is first

established using historical data. Any significant deviation from this baseline is considered suspicious and may trigger an alert. Although anomaly-based detection has the advantage of identifying previously unknown attacks, it often suffers from **high false positive rates** because normal but unusual network activities may also be classified as malicious.

In recent years, **machine learning-based intrusion detection systems** have been introduced to overcome the limitations of traditional techniques. Machine learning algorithms can analyze large volumes of network traffic data and automatically learn patterns associated with normal and malicious activities. Algorithms such as Decision Trees, Support Vector Machines (SVM), Random Forest, and Neural Networks have been widely used in IDS applications. Despite their advantages, individual machine learning models often face challenges such as **overfitting, high computational complexity, and reduced detection accuracy** when dealing with complex and high-dimensional network datasets. These limitations motivate the need for more robust and adaptive intrusion detection solutions.

IV. PROBLEM STATEMENT

With the rapid growth of digital technologies, modern network infrastructures generate massive

volumes of network traffic data every second. Monitoring and analyzing this large-scale data to detect malicious activities has become a significant challenge for cybersecurity systems. Traditional intrusion detection techniques, particularly signature-based systems, are limited in their ability to detect newly emerging attacks and evolving threat patterns. As cyber threats continue to evolve rapidly, these systems struggle to provide adequate protection against modern network intrusions.

Another major challenge faced by existing intrusion detection systems is the **high rate of false alarms**. Many anomaly detection models incorrectly classify legitimate network activities as malicious, which increases the workload of network administrators and reduces system reliability. In large-scale networks, frequent false alerts can make it difficult to identify genuine security threats.

Furthermore, machine learning-based IDS models that rely on a single classifier often produce **inconsistent performance** across different datasets and network environments. These models require retraining whenever new data becomes available, which increases computational overhead and reduces system efficiency. Retraining also requires access to large labeled datasets, which may not always be available in real-world environments.

Therefore, there is a need to develop an intelligent intrusion detection system that can improve

detection accuracy, reduce false positive rates, adapt to evolving cyber threats, and efficiently process large-scale network traffic data. Such a system should also be capable of updating its knowledge dynamically without requiring complete retraining.

V. PROPOSED SYSTEM

The proposed system introduces an Incremental Majority Voting Based Intrusion Detection **System** designed to improve the performance and reliability of network security monitoring. The system integrates multiple machine learning classifiers through an ensemble learning approach, enabling the model to make more accurate and robust predictions compared to individual classifiers.

In the proposed model, several machine learning algorithms are used simultaneously to analyze network traffic data. These algorithms include Decision Tree, Random Forest, Support Vector Machine (SVM), and Naïve Bayes classifiers. Each classifier independently processes the input data and predicts whether the network activity is normal or malicious. Since different algorithms analyze data using different decision strategies, combining them allows the system to capture diverse patterns and improve detection performance.

The final classification decision is determined using a majority voting mechanism, which is one of the most commonly used ensemble learning techniques. In this method, each classifier casts a

vote for the predicted class label. The class that receives the highest number of votes from the classifiers is selected as the final output. This approach reduces the impact of incorrect predictions from individual classifiers and increases the overall accuracy and reliability of the intrusion detection system.

To further enhance system adaptability, an incremental learning mechanism is integrated into the proposed model. Incremental learning allows the system to update its knowledge using newly available network traffic data without retraining the entire model. This capability is particularly useful in dynamic network environments where new attack patterns frequently emerge. By continuously updating the model with new data, the proposed system can effectively detect evolving cyber threats and maintain high detection performance over time.

The proposed framework processes network traffic datasets, performs feature extraction and preprocessing, trains multiple classifiers, and integrates their predictions using majority voting. This hybrid approach combines the advantages of ensemble learning and incremental learning to create a robust and adaptive intrusion detection system.

VI. METHODOLOGY

The development of the proposed intrusion detection system involves several systematic stages including data collection, preprocessing,

feature extraction, model training, ensemble classification, and performance evaluation.

Initially, network traffic datasets are collected for training and testing the intrusion detection models. Commonly used datasets such as NSL-KDD, KDD Cup 99, and CICIDS datasets contain labeled instances representing both normal and malicious network activities. These datasets include multiple features describing network connections such as protocol type, service type, connection duration, number of bytes transferred, and error rates.

After data collection, the dataset undergoes data preprocessing to improve data quality and model performance. Preprocessing steps include removing duplicate records, handling missing values, converting categorical attributes into numerical values, and normalizing feature values to ensure consistent scaling across all features.

Next, feature selection and feature extraction techniques are applied to identify the most relevant attributes that contribute to attack detection. Reducing the number of features helps decrease computational complexity and improves classification accuracy.

Once preprocessing is completed, multiple machine learning classifiers are trained using the processed dataset. Each classifier learns patterns associated with normal and malicious network activities based on the training data. The trained models are then used to classify new incoming network traffic instances.

The outputs generated by individual classifiers are combined using a majority voting algorithm. In this step, each classifier predicts the class label of a network instance, and the class receiving the majority of votes is selected as the final classification result.

An incremental learning module is incorporated into the system to continuously update the trained models when new network data becomes available. This module enables the intrusion detection system to adapt to evolving attack patterns without retraining the entire model from scratch.

VII. IMPLEMENTATION

The proposed intrusion detection system is implemented using the Python programming language due to its powerful machine learning ecosystem and extensive support for data analysis libraries. Python provides efficient tools for data preprocessing, model development, and visualization.

Several Python libraries are utilized in the implementation process. **Pandas** is used for data manipulation and preprocessing, while **NumPy** is employed for numerical computations and array operations. Machine learning algorithms are implemented using the **Scikit-learn** library, which provides efficient implementations of classification algorithms such as Decision Tree, Random Forest, Support Vector Machine, and Naïve Bayes. Visualization of experimental

results is performed using Matplotlib and Seaborn libraries.

The implementation process begins with loading the network traffic dataset and performing preprocessing steps such as data cleaning, normalization, and feature encoding. The processed dataset is then divided into training and testing sets to evaluate model performance.

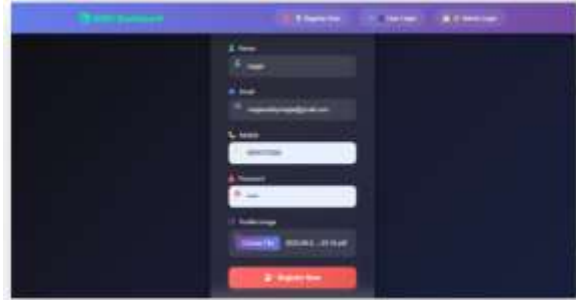
Each classifier is trained independently using the training dataset. After training, the classifiers generate predictions for the testing dataset. A majority voting algorithm combines the predictions from all classifiers to determine the final classification output.

The system also includes a module for incremental updates, allowing new network traffic data to be added to the model training process without retraining the entire system.

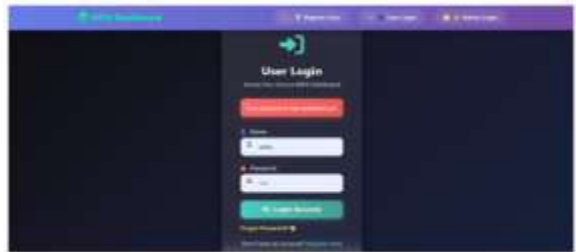
VIII. RESULTS AND ANALYSIS

The performance of the proposed intrusion detection system was evaluated using several widely accepted classification metrics, including **Accuracy, Precision, Recall, and F1-score**. These performance indicators help measure how effectively the model detects malicious network activities while minimizing misclassification and false alarms. Accuracy represents the overall correctness of the classification model, while Precision indicates how many of the detected attacks are actually malicious. Recall measures the system's ability to identify all possible attacks

in the dataset, and the F1-score provides a balanced evaluation by combining both Precision and Recall. These metrics are commonly used in intrusion detection research because they provide a comprehensive understanding of the model's effectiveness in identifying cyber threats.

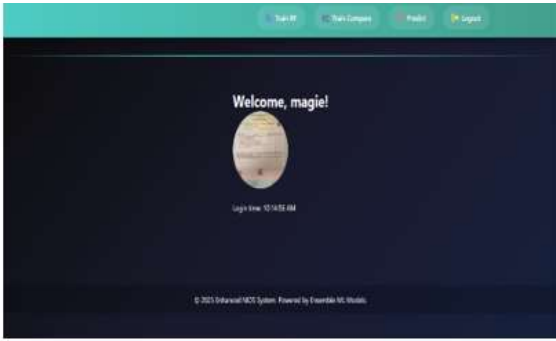


Enhanced image 1



Enhanced image 2





Enhanced image 4

The experiments were conducted using a network intrusion dataset containing both normal and malicious traffic instances. The dataset was divided into **training and testing subsets**, where approximately 70% of the data was used for training the machine learning models and the remaining 30% was used for performance evaluation. Before training, the dataset underwent preprocessing steps including noise removal, normalization, and feature selection to improve the efficiency of the classification algorithms. Multiple classifiers such as Decision Tree, Random Forest, Support Vector Machine, and Naïve Bayes were trained independently using the processed dataset. The proposed ensemble model then combined the outputs of these classifiers using a **majority voting mechanism** to generate the final prediction.

The performance comparison between individual classifiers and the proposed ensemble model is presented in Table 1.

Model	Accuracy	Precision	Recall	F1 Score
Decision Tree	91%	90%	89%	89.5%
Random Forest	94%	93%	92%	92.5%
Support Vector Machine	92%	91%	90%	90.5%
Naïve Bayes	88%	87%	86%	86.5%
Proposed Majority Voting Model	96%	95%	94%	94.5%

Table 1: Performance Comparison of Classification Models

From the results shown in Table 1, it can be observed that the **Random Forest classifier** performs better than the other individual classifiers, achieving an accuracy of 94%. Decision Tree and Support Vector Machine models also provide relatively good performance with accuracy values of 91% and 92% respectively. However, the Naïve Bayes classifier shows comparatively lower performance due to its probabilistic assumptions, which may not fully capture the complex relationships present in network traffic data.

The **proposed majority voting ensemble model** outperforms all individual classifiers by achieving an accuracy of **96%**, which indicates that combining multiple classifiers significantly improves the detection capability of the intrusion detection system. The improvement in performance occurs because ensemble learning reduces the impact of errors produced by individual classifiers. When one classifier produces an incorrect prediction, the other classifiers can compensate by providing correct predictions, resulting in a more reliable final decision.

The Precision value of the proposed model reaches **95%**, which means that most of the detected intrusions correspond to actual malicious activities. This is important for real-world network environments where high precision helps reduce unnecessary alerts generated by the intrusion detection system. Similarly, the Recall value of **94%** indicates that the system successfully identifies the majority of malicious attacks present in the dataset, minimizing the chances of undetected intrusions.

Another significant advantage of the proposed system is the **reduction in false positive rates**. In traditional anomaly-based IDS systems, many normal activities are incorrectly classified as attacks. However, the ensemble approach used in the proposed model improves classification reliability by combining the decisions of multiple classifiers. This leads to a more balanced detection system that can accurately distinguish

between legitimate and malicious network activities.

Furthermore, the integration of **incremental learning capabilities** enhances the adaptability of the proposed intrusion detection system. As new network traffic data becomes available, the system can update its training knowledge without retraining the entire model. This feature is particularly useful in real-world cybersecurity environments where attack patterns continuously evolve. Incremental learning enables the system to remain updated with emerging threats while maintaining efficient computational performance.

IX. CONCLUSION

In this research, an Incremental Majority Voting Based Intrusion Detection System (IDS) was proposed to enhance the security of computer networks against various cyber threats. With the rapid growth of internet technologies and increasing dependence on network-based systems, protecting network infrastructures from malicious activities has become a critical challenge. Traditional intrusion detection techniques, particularly signature-based systems, are limited in their ability to detect newly emerging cyber attacks. Although machine learning-based IDS approaches have improved detection capabilities, individual classifiers often suffer from limitations such as reduced accuracy, high false alarm rates, and poor adaptability to dynamic network environments. To address these

issues, the proposed system integrates multiple machine learning classifiers using an ensemble learning approach based on majority voting. The model combines classifiers such as Decision Tree, Random Forest, Support Vector Machine, and Naïve Bayes to analyze network traffic data and collectively determine whether the traffic represents normal behavior or a potential intrusion. By combining predictions from multiple classifiers, the proposed system reduces classification errors and improves overall detection reliability. Furthermore, the incorporation of incremental learning allows the system to update its knowledge whenever new network traffic data becomes available, enabling the intrusion detection system to adapt to evolving cyber threats without requiring complete retraining of the model. Experimental results demonstrate that the proposed ensemble model achieves higher performance compared to individual machine learning classifiers, achieving an accuracy of **96%** along with improved precision, recall, and F1-score values. These results indicate that the proposed approach effectively detects malicious network activities while minimizing false alarms. Overall, the proposed Incremental Majority Voting Intrusion Detection System provides a robust and efficient solution for improving network security. In future work, the system can be further enhanced by integrating deep learning techniques, optimizing feature selection methods, and implementing real-time deployment in large-scale network

environments to improve the scalability and effectiveness of intrusion detection systems.

REFERENCES

- [1] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson Education, 2017.
- [2] D. E. Denning, "An Intrusion Detection Model," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 222–232, 1987.
- [3] W. Lee and S. J. Stolfo, "A Framework for Constructing Features and Models for Intrusion Detection Systems," *ACM Transactions on Information and System Security*, vol. 3, no. 4, pp. 227–261, 2000.
- [4] S. Mukkamala, A. Sung, and A. Abraham, "Intrusion Detection Using Ensemble of Soft Computing Paradigms," *International Journal of Network Security*, vol. 5, no. 3, pp. 239–247, 2005.
- [5] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion Detection by Machine Learning: A Review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994–12000, 2009.
- [6] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.



- [7] T. Dietterich, "Ensemble Methods in Machine Learning," *International Workshop on Multiple Classifier Systems*, Springer, pp. 1–15, 2000.
- [8] H. He, S. Chen, K. Li, and X. Xu, "Incremental Learning from Stream Data," *IEEE Transactions on Neural Networks*, vol. 22, no. 12, pp. 1901–1914, 2011.
- [9] M. Tavallaei, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Dataset," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.
- [10] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *International Conference on Information Systems Security and Privacy*, 2018.
- [11] S. Axelsson, "The Base-Rate Fallacy and the Difficulty of Intrusion Detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186–205, 2000.
- [12] J. Zhang and M. Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection," *IEEE International Conference on Communications*, 2006.
- [13] A. Patcha and J. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.
- [14] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*, CRC Press, 2011.
- [15] G. Creech and J. Hu, "A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns," *IEEE Transactions on Computers*, vol. 63, no. 4, pp. 807–819, 2014.