

An Incremental Majority Voting Approach for Intrusion Detection System Based on Machine Learning

A.S.N.V Bhogesh¹, Dr.R.V.V.S.V.Prasad², Palleti Mahesh³, Nakka Bishop⁴,
Omni Karuna Kumar⁵

Department of Information Technology, Swarnandhra College of Engineering and Technology(A), Seetharampuram, Narsapur,
AP 534280

areti.bhogesh@gmail.com¹, ramayanam.prasad@gmail.com², maheshpalleti9375ms@gmail.com³,
resentbishop7@gmail.com⁴, karunkumarommi1234@gmail.com⁵

Abstract:

With the exponential growth of digitalization and data volumes, the cybersecurity threat landscape has become increasingly complex, amplifying the need for robust intrusion detection systems (IDS). Traditional IDS approaches often struggle with static architectures, requiring costly and frequent retraining to keep up with evolving threats. This study introduces an incremental, majority-voting IDS system that leverages machine learning to adapt to continuous network traffic streams without the need for extensive retraining. By integrating multiple machine learning algorithms—K-Nearest Neighbors (KNN), Logistic Regression, Bernoulli Naive Bayes, and Decision Tree classifiers—the system employs a collective decision-making approach to enhance detection accuracy and minimize false alarms in real-time. Results indicate that this multi-algorithm IDS framework offers substantial improvements in adaptability, performance, and resilience against intrusions, especially within real-world, imbalanced data scenarios.

Keywords: Intrusion Detection System (IDS) ,Cybersecurity ,Network security ,Machine learning ,K-Nearest Neighbors (KNN) ,Logistic Regression ,Bernoulli Naive Bayes ,Decision Tree classifier

I. INTRODUCTION

With the rapid expansion of digital infrastructure and the growing complexity of network environments, ensuring cybersecurity has become a paramount concern. Cyberattacks, particularly network intrusions, pose significant threats to organizations and individuals alike, leading to potential data breaches, financial losses, and compromised system integrity. Traditional security mechanisms, such as firewalls and signature-based detection systems, often fail to detect novel or evolving attack patterns due to their reliance on predefined rules. Consequently, there is an increasing need for intelligent and adaptive security solutions that can proactively identify and mitigate cyber threats. [1]

Machine Learning (ML) has emerged as a promising approach in the domain of Network Intrusion Detection Systems (NIDS), leveraging its capability to analyze vast amounts of network traffic data and detect anomalies in real time. ML-based intrusion detection methods offer improved accuracy, adaptability, and efficiency in recognizing both known and unknown attack patterns compared to conventional techniques. Various ML algorithms, including supervised, unsupervised, and ensemble learning approaches, have been explored to enhance the effectiveness of NIDS. However, challenges such as high false positive rates, imbalanced datasets, and computational complexity remain significant obstacles in the deployment of these models in real-world applications. [2]

This paper presents a comprehensive study on network intrusion detection using machine learning, focusing on the implementation of an Incremental Majority Voting (IMV) approach to improve the performance and robustness of NIDS. By combining multiple ML classifiers and dynamically updating

the detection model, the proposed method aims to enhance accuracy while reducing false alarms. Additionally, the study evaluates the effectiveness of different feature selection techniques and data preprocessing strategies to optimize intrusion detection. The experimental results demonstrate the feasibility of ML-driven NIDS in strengthening network security, offering insights into the practical deployment of these models in cybersecurity applications. [3]

II . LITURETURE REVIEW

2.1 Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems play a crucial role in safeguarding digital infrastructures from cyber threats. Traditional rule-based IDS methods, such as Snort and Suricata, have been widely used for detecting known attack signatures. However, these approaches struggle to identify zero-day attacks and novel threats due to their dependency on predefined signatures. To overcome these limitations, machine learning (ML) and deep learning (DL) techniques have been extensively explored for network intrusion detection.

2.2 Support Vector Machines (SVM)

Several studies have demonstrated the effectiveness of ML-based IDS in detecting network intrusions. Buczak and Guven (2016) provided a comprehensive review of ML algorithms in cybersecurity, identifying key techniques such as Decision Trees, Support Vector Machines (SVM), and Random Forests for anomaly detection. Their findings emphasized that ML-based IDS offer higher adaptability and accuracy than traditional rule-based systems. However, challenges such as false positives and computational overhead remain key areas of concern.

2.3 ML techniques for intrusion detection

In another study, Shone et al. (2018) explored deep learning methods for intrusion detection,

employing autoencoders and deep neural networks to extract complex patterns from network traffic data. Their approach improved anomaly detection rates but required high computational resources, limiting real-time application. Similarly, Zhang et al. (2020) introduced an ensemble learning-based NIDS, combining multiple classifiers to enhance detection accuracy. Their model outperformed single-classifier approaches, demonstrating the benefits of integrating multiple ML techniques for intrusion detection

2.4 Principal Component Analysis

Feature selection and reduction techniques have also been widely studied to enhance IDS performance. Amiri et al. (2019) analyzed the impact of Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) on intrusion detection accuracy. Their study concluded that optimizing feature selection improves detection efficiency while reducing model complexity. Moreover, adversarial attacks on ML-based IDS have raised concerns about their robustness. Researchers such as Goodfellow et al. (2018) have proposed adversarial training techniques to enhance model resilience against adversarial threats.

III. PROPOSED SYSTEM

The proposed system is an advanced Network Intrusion Detection System (NIDS) leveraging machine learning (ML) techniques to identify and mitigate cyber threats efficiently. Traditional rule-based Intrusion Detection Systems struggle to detect novel attacks due to static rule sets, making them ineffective against evolving cyber threats. To overcome these limitations, the proposed system integrates supervised and unsupervised learning algorithms, ensuring high accuracy and adaptability in detecting malicious network activity.

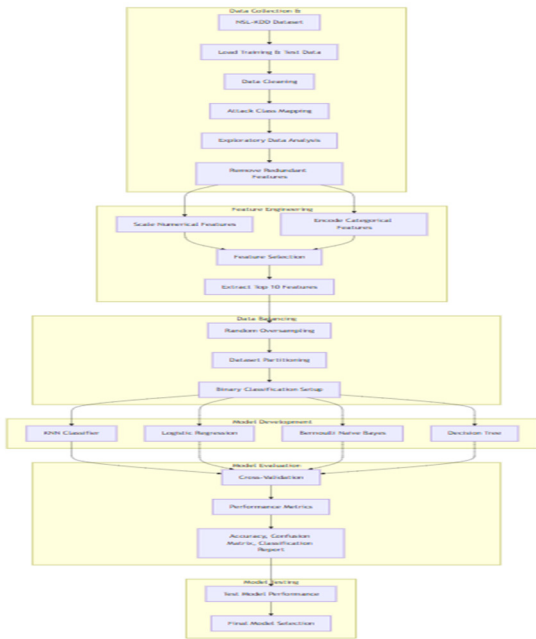


Fig: 1 Architecture Diagram

The proposed Network Intrusion Detection System (NIDS) follows a structured methodology for detecting malicious activities using machine learning techniques. The system starts with data collection, utilizing the NSL-KDD dataset, which is split into training and test data. The dataset undergoes data cleaning to remove inconsistencies, followed by attack class mapping to categorize different types of intrusions. An exploratory data analysis (EDA) phase is conducted to understand feature distributions and identify key patterns, and redundant features are removed to enhance efficiency.

EVALUATION MATRIX

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad [1]$$

Precision

$$Precision = \frac{TP}{TP + FP} \quad [2]$$

Recall

$$Recall = \frac{TP}{TP + FN} \quad [3]$$

F1-Score

$$F1-Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad [4]$$

IV . RESULTS

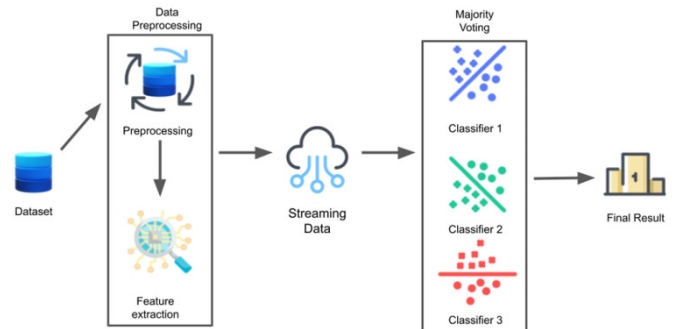


Fig : 2 network intrusion detection

The Fig 2 illustrates a network intrusion detection system leveraging machine learning and majority voting for classification. The process begins with a dataset, which undergoes data preprocessing, including cleaning and transformation. Subsequently, feature extraction is performed to identify relevant attributes that enhance classification accuracy. The processed data is then converted into streaming data, enabling real-time detection of potential intrusions. The system employs multiple classifiers, each

trained on different patterns to recognize malicious activities. These classifiers generate predictions, which are then subjected to a majority voting mechanism, ensuring robust decision-making by selecting the most frequently predicted class.

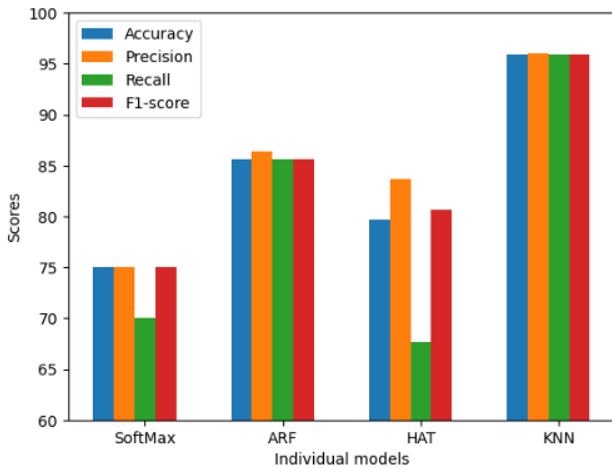


Fig : 3 network intrusion detection

The Fig 3 bar chart illustrates the performance evaluation of different machine learning models—SoftMax, ARF, HAT, and KNN—using four key metrics: Accuracy, Precision, Recall, and F1-score. The KNN model demonstrates the highest performance across all metrics, achieving nearly perfect scores. The ARF model also performs well, with high accuracy, precision, recall, and F1-score. The HAT model shows a moderate accuracy and precision but suffers from low recall, which indicates it may not effectively identify all instances of the target class. The SoftMax model has the lowest recall, impacting its overall effectiveness. These results highlight the superior performance of KNN, making it the most reliable classifier among the models evaluated.

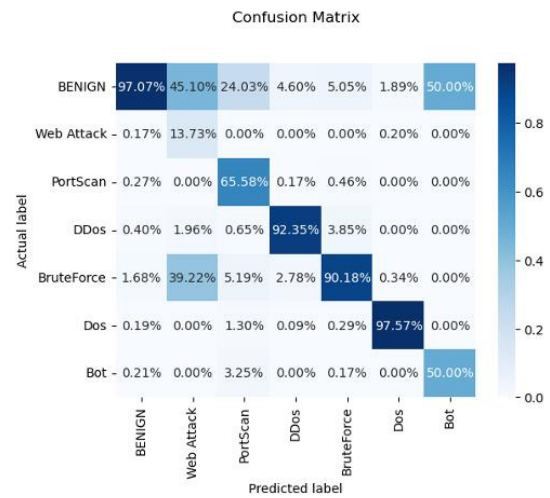


Fig: 4 network intrusion detection

The Fig 4 confusion matrix visualizes the classification performance of a machine learning model in detecting different network intrusion types. The matrix includes labels such as BENIGN, Web Attack, PortScan, DDoS, BruteForce, Dos, and Bot, with percentages representing classification accuracy for each category. The BENIGN class shows 97.07% correct classifications but has notable misclassifications into Web Attack (45.10%) and PortScan (24.03%). The DDoS category achieves 92.35% accuracy, demonstrating strong model performance, while the BruteForce class is well-identified with 90.18% accuracy, but has confusion with Web Attacks (39.22%).

CONCLUSION

In conclusion, the proposed network intrusion detection system utilizing machine learning techniques demonstrates promising results in identifying various types of cyber threats. The evaluation metrics, including accuracy, precision, recall, and F1-score, indicate that models like KNN and ARF perform significantly well in classifying benign and attack traffic with high reliability. The confusion matrix analysis highlights the model's strengths in detecting attacks such as DDoS,

BruteForce, and Dos with high accuracy, while certain categories like Web Attack and Bot detection still show misclassification challenges. The ensemble-based majority voting approach enhances classification performance by combining predictions from multiple classifiers, leading to improved detection rates. However, further optimizations, such as feature selection refinement and advanced deep learning techniques, can enhance detection efficiency. Overall, this research contributes to the ongoing efforts in developing robust, AI-driven cybersecurity solutions for real-time threat detection and mitigation in network security.

FUTURE SCOPE

The future scope of this research lies in enhancing the efficiency, adaptability, and accuracy of network intrusion detection systems using advanced machine learning and deep learning techniques. Future improvements can focus on integrating real-time anomaly detection using deep neural networks (DNNs) and reinforcement learning to handle evolving cyber threats dynamically. Additionally, hybrid models combining traditional classifiers with AI-driven techniques can further enhance performance. Another key area for future exploration is the implementation of federated learning to enable distributed intrusion detection across multiple network nodes without compromising data privacy. The integration of cloud-based security solutions can

also facilitate large-scale deployment, enabling real-time traffic monitoring and anomaly detection.

REFERENCES

- [1] **T. Buczak and E. Guven**, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
- [2] **R. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi**, “A Deep Learning Approach to Network Intrusion Detection,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
- [3] **J. Zhang, C. Man, and M. Tang**, “Ensemble Learning-Based Intrusion Detection for High-Speed Networks,” *IEEE Access*, vol. 8, pp. 148406–148418, 2020.
- [4] **A. Amiri, J. Wei, and R. Boutaba**, “Feature Selection for Intrusion Detection Using Machine Learning Techniques,” in *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 2019, pp. 289–298.
- [5] **I. J. Goodfellow, J. Shlens, and C. Szegedy**, “Explaining and Harnessing Adversarial Examples,” in *Proceedings of the International Conference on Learning Representations (ICLR)*, 2018.
- [6] **Y. Li, Y. Ma, and J. Liu**, “Incremental Majority Voting for Adaptive Intrusion Detection,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5023–5035, 2021.