IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

Machine Learning-Driven Network Intrusion Detection: An Intelligent Approach

Mr.G.Vijay Kumar[1], Gajarao Meghana Sri Sai Satya Sri[2], Sripada S Sai Subrahmanya Kireeti[3], Kurre Anitha[4] ,Racha Mohan Durga Venkata Narayana[5] ,Satya Charan Kandula[6].

vijay9908914010@gmail.com[1],gajaraomeghana@gmail.com[2] kireetis10@gmail.com[3], anithakurre516@gmail.com[4] , Mohan.student51@gmail.com[5] , satyacharan9595@gmail.com[6] .

"Pragati Engineering College 1-378, ADB Road, Surampalem Near Kakinada, Surampalem, Andhra Pradesh 533455"

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

INTRODUCTION

With the exponential increase in digitalization and data generation, the cybersecurity landscape is continuously evolving, presenting new challenges for network security. Intrusion Detection Systems (IDS) play a crucial role in safeguarding networks against malicious attacks, unauthorized access, and cyber threats. Traditional IDS models often rely on static architectures that require periodic retraining, making them inefficient in handling emerging attacks and dynamic network environments. [1]

To address these challenges, researchers have explored machine learning-based IDS frameworks that can adapt to evolving threats in real time. However, existing solutions often suffer from issues such as high false alarm rates, computational inefficiencies, and an inability to handle imbalanced data effectively. Additionally, conventional IDS models struggle with concept drift, where the statistical properties of incoming network traffic change over time, leading to performance degradation.[2]

Recent advancements in ensemble learning and incremental learning have demonstrated significant potential in overcoming these limitations. By leveraging multiple machine learning algorithms in a majority voting-based ensemble, IDS can achieve higher accuracy, reduced

false positives, and improved adaptability. In particular, techniques such as K-Nearest Neighbors (KNN), Softmax Regressor, Adaptive Random Forest (ARF), and Hoeffding Adaptive Tree (HAT) have shown promising results in enhancing IDS performance by dynamically adjusting to evolving attack patterns. [3]

This paper introduces an Incremental Majority Voting Approach for an Intrusion Detection System based on Machine Learning. The proposed model integrates multiple classifiers to improve detection accuracy while mitigating issues related to imbalanced data and concept drift. Using a well-curated dataset, such as CICIDS2017, this study evaluates the efficacy of the proposed approach in real-world scenarios. The experimental results indicate that the ensemble model significantly outperforms traditional IDS frameworks, demonstrating robustness, scalability, and practical applicability in modern cybersecurity infrastructures. [4]

The remainder of this paper is organized as follows: Section II reviews related works in IDS and machine learning-based intrusion detection. Section III presents the methodology and details of the proposed approach. Section IV discusses experimental results and performance evaluations. Finally, Section V concludes the paper with key findings and future research directions. [5]

II . LITURETURE SURVEY

1. Mijwil et al. (2023) conducted an in-depth analysis of the top five evolving cybersecurity threats. Their study highlights the increasing sophistication of cyber threats and their impact on individuals, organizations, and governments. The paper explores various attack vectors, including ransomware, phishing, advanced persistent threats (APTs), and other emerging cybersecurity challenges.
2. Fadziso et al. (2023) provided an overview of the scale of cyber threats and how they have evolved over time. Their research discusses how digitalization has led to new attack surfaces, making cybersecurity more complex. They emphasize the importance of proactive security measures to mitigate the growing risks associated with cyber threats.
3. Dillon et al. (2021) examined the changing landscape of cybersecurity in a post-COVID-19 world. Their work, included in a book on digital transformation, discusses how the pandemic accelerated digital adoption, thereby increasing vulnerabilities. They highlight various emerging threats and the need for sustainable innovation and adaptive security strategies to counter these risks.
4. Vanin et al. (2022) conducted a study on network intrusion detection systems (IDS) using artificial intelligence and machine learning techniques. Their research focuses on how AI-powered IDS can improve threat detection by analyzing patterns and anomalies in network traffic. They emphasize the advantages of machine learning in enhancing cybersecurity defenses.

5. Albasheer et al. (2022) explored cyber-attack prediction using network intrusion detection systems and alert correlation techniques. Their survey examines how integrating AI with IDS can enhance the ability to detect and respond to threats in real time. The study also discusses different methodologies for improving cybersecurity by predicting and mitigating potential attacks before they occur.
6. Ahmad et al. (2021) conducted a systematic study on network intrusion detection systems (NIDS) utilizing machine learning and deep learning techniques. Their research, published in Transactions on Emerging Telecommunications Technologies, evaluates various ML and DL approaches, comparing their effectiveness in identifying cyber threats. The study highlights the importance of AI-driven methodologies in enhancing the accuracy and efficiency of intrusion detection.
7. Liu and Lang (2019) provided a comprehensive survey on machine learning and deep learning methods for intrusion detection systems (IDS). Published in Applied Sciences, their work reviews different AI-based approaches, discussing their strengths and limitations. The authors emphasize the role of ML and DL in improving threat detection, reducing false alarms, and automating cybersecurity processes.
8. Shahbandayeva et al. (2022) explored network intrusion detection using both supervised and unsupervised machine learning techniques. Presented at the 16th IEEE International Conference on Applied Information and Communication Technology (AICT), their study compares the performance of various ML models in detecting cyber threats. The research highlights how combining supervised and unsupervised learning can improve intrusion detection accuracy.
9. Gamage and Samarabandu (2020) conducted a survey and comparative study on deep learning methods in network intrusion detection. Published in the Journal of Network and Computer Applications, their research analyzes different DL approaches, assessing their efficiency in handling complex cyber threats. The study provides an objective comparison of DL-based IDS models, focusing on their scalability and real-time threat detection capabilities.
10. Adewole et al. (2022) performed an empirical analysis of data streaming and batch learning models for network intrusion detection. Published in Electronics, their study investigates the performance of real-time data processing techniques in detecting cyber threats. The authors emphasize the advantages of streaming-based IDS models in identifying and mitigating attacks with minimal latency.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

III. PROPOSED SYSTEM

With the increasing complexity of cyber threats, traditional Intrusion Detection Systems (IDS) are no longer sufficient. Static IDS models require frequent retraining and struggle to adapt to evolving threats. To address these challenges, we propose an Incremental Majority Voting-Based IDS that leverages machine learning to dynamically learn from network traffic streams, improve detection accuracy, and minimize false alarms.

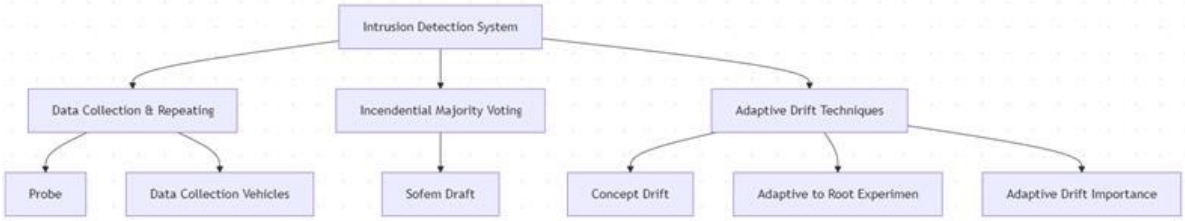

FIG : 1 Architecture Diagram

The Intrusion Detection System (IDS) Architecture comprises three main components: Data Collection & Repeating, Incremental Majority Voting, and Adaptive Drift Techniques. The Data Collection & Repeating module is responsible for continuously gathering network traffic data to detect anomalies. It includes Probe, which identifies suspicious activities and scans network vulnerabilities, and Data Collection Vehicles, which ensure systematic data acquisition for further analysis. The Incremental Majority Voting component enhances intrusion detection accuracy by integrating multiple classifiers, where the Sofem Draft refines the voting mechanism and improves decision-making. Lastly, the Adaptive Drift Techniques module helps the system adjust to evolving cyber threats by handling Concept Drift, which enables dynamic model updates in response to new attack patterns.

IV. EVALUATION MATRICS

Accuracy

Measures the percentage of correctly classified instances (both attacks and normal traffic)

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

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

TP (True Positives): Correctly detected attacks.

TN (True Negatives): Correctly identified normal traffic.

FP (False Positives): Normal traffic misclassified as an attack.

FN (False Negatives): Attacks misclassified as normal traffic.

Precision (Positive Predictive Value)

Determines how many of the detected attacks are actual attacks.

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

Recall (Detection Rate or Sensitivity)

Measures the system's ability to correctly identify attacks from all actual attack instances.

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

F1-Score

Balances Precision and Recall by computing their harmonic mean.

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

V . RESULTS

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

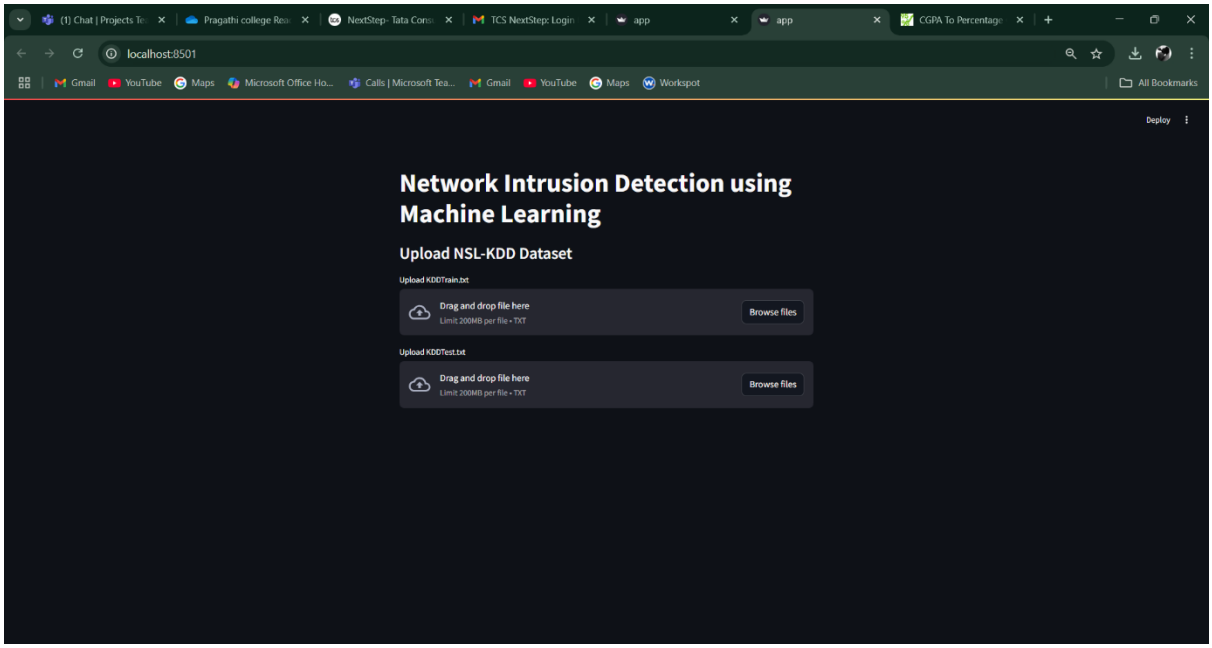

Fig: 5.1 Network_Intrusion_Detection

The interface shown in the image represents a Network Intrusion Detection System (NIDS) using Machine Learning, designed for detecting cyber threats based on the NSL-KDD dataset. The webpage provides an option to upload two essential files: KDDTrain+.txt for training the machine learning model and KDDTest+.txt for testing its accuracy and performance. The interface includes a drag-and-drop feature along with a Browse files button, making it easy for users to upload large datasets, with a limit of 200MB per file in .txt format.

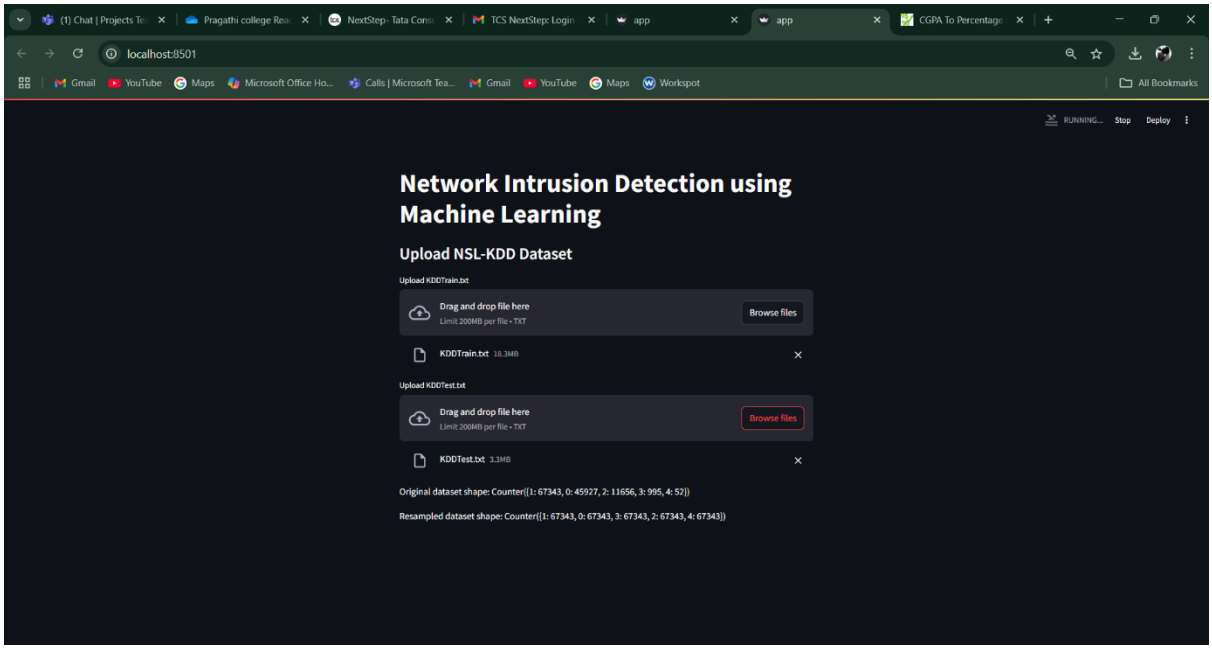

Fig: 5.2 Network_Intrusion_Detection_Dataset

The interface displayed represents a Network Intrusion Detection System (NIDS) using Machine Learning, where users can upload the NSL-KDD dataset for training and testing the

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

model. The system allows uploading two files: KDDTrain.txt (18.3MB) for training and KDDTest.txt (3.3MB) for testing. The UI includes a drag-and-drop feature and a Browse files button, enabling easy dataset uploads, with a 200MB per file limit in .txt format.

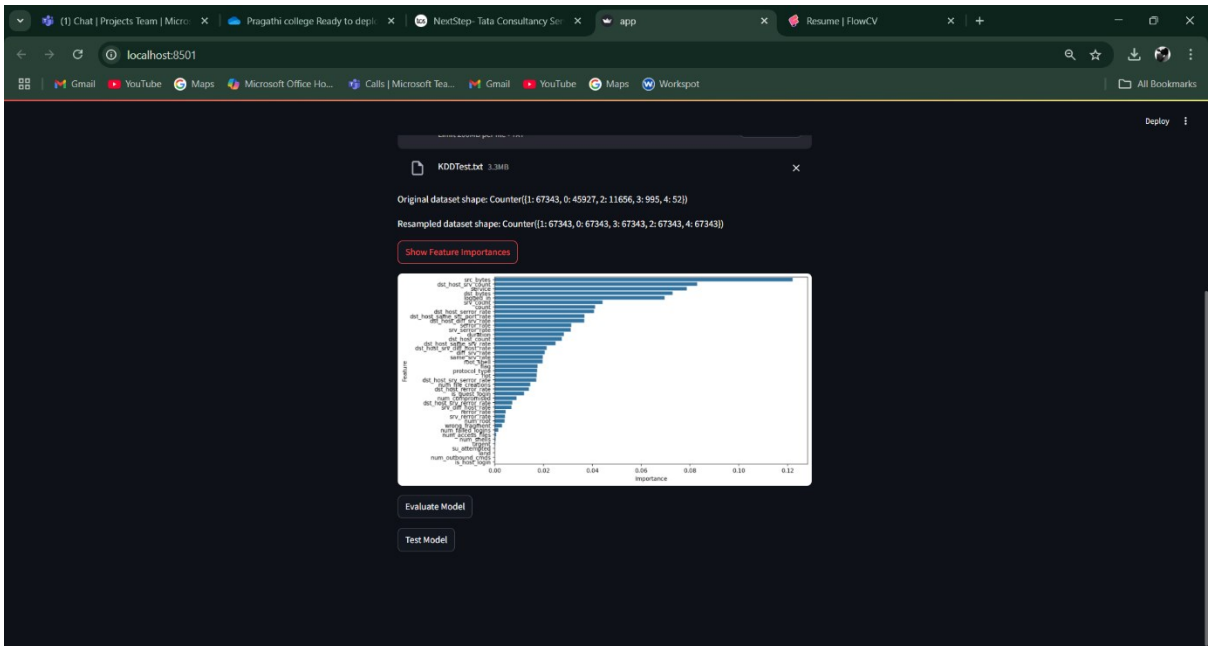

Fig: 5.3 Network Intrusion Detection System (NIDS)

The image showcases a Network Intrusion Detection System (NIDS) using Machine Learning, where the system processes the NSL-KDD dataset to detect malicious network activities. It presents the original and resampled dataset distributions, ensuring balanced data for improved model performance. A feature importance graph is displayed, highlighting the most influential factors in intrusion detection. Additionally, options like "Evaluate Model" and "Test Model" indicate that users can assess and validate the machine learning model's effectiveness in identifying threats.

CONCLUSION

The Network Intrusion Detection System (NIDS) using Machine Learning presents a robust approach to identifying and mitigating network threats. By leveraging the NSL-KDD dataset and implementing techniques like incremental majority voting and adaptive drift handling, the system improves detection accuracy and adaptability to evolving cyber threats. The feature importance analysis ensures that the model focuses on the most relevant attributes, enhancing overall efficiency. The evaluation of various machine learning algorithms allows for optimizing performance, making the system a reliable cybersecurity solution.

FUTURE SCOPE

For the future scope, the system can be enhanced by integrating deep learning techniques such as recurrent neural networks (RNNs) or transformers for better anomaly detection. Real-time intrusion detection with automated threat response mechanisms could significantly reduce reaction time to cyber-attacks. Additionally, incorporating federated learning can enable decentralized intrusion detection without compromising data privacy. Expanding the dataset to

include more modern attack types and utilizing cloud-based deployment would further improve scalability and adaptability in enterprise security environments.

REFERENCES

1. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: An in-depth overview," Mesopotamian Journal of Cyber Security, vol. 2023, pp. 57–63, Mar. 2023.
2. T. Fadziso, U. Thaduri, S. Dekkati, V. Ballamudi, and H. Desamsetti, "Evolution of the cyber security threat: An overview of the scale of cyber threat," Digitalization Sustainability Review, vol. 3, no. 1, pp. 1–12, 2023.
3. R. Dillon, P. Lothian, S. Grewal, D. Pereira, and A. Kuah, "Cyber security: Evolving threats in an ever-changing world," in Digital Transformation in a Post-Covid World: Sustainable Innovation, Disruption and Change. Boca Raton, FL, USA: CRC Press, 2021, pp. 129–154.
4. P. Vanin, T. Newe, L. L. Dhirani, E. O'Connell, D. O'Shea, B. Lee, and M. Rao, "A study of network intrusion detection systems using artificial intelligence/machine learning," Applied Sciences, vol. 12, no. 22, p. 11752, Nov. 2022, doi: 10.3390/app122211752.
5. H. Albasheer, M. Md Siraj, A. Mubarakali, O. Elsier Tayfour, S. Salih, M. Hamdan, S. Khan, A. Zainal, and S. Kamarudeen, "Cyber attack prediction based on network intrusion detection systems for alert correlation techniques: A survey," Sensors, vol. 22, no. 4, p. 1494, Feb. 2022.
6. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, Jan. 2021.
7. H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," Applied Sciences, vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.
8. L. Shahbandayeva, U. Mammadzada, I. Manafova, S. Jafarli, and A. Z. Adamov, "Network intrusion detection using supervised and unsupervised machine learning," in Proceedings of the IEEE 16th International Conference on Applied Information and Communication Technologies (AICT), Oct. 2022, pp. 1–7.
9. S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," Journal of Network and Computer Applications, vol. 169, Nov. 2020, Art. no. 102767. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520302411
10. K. S. Adewole, T. T. Salau-Ibrahim, A. L. Imoize, I. D. Oladipo, M. AbdulRaheem, J. B. Awotunde, A. O. Balogun, R. M. Isiaka, and T. O. Aro, "Empirical analysis of data streaming and batch learning models for network intrusion detection," Electronics, vol. 11, no. 19, p. 3109, Sep. 2022.