Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

Optimizing Network Intrusion Detection through Deep Learning and Class Imbalance Mitigation

MR.K. UDAY KIRAN[1], KETHUBOINA.SAIKUMAR[2]

#1 Assistant Professor Department of Master of Computer Application
#2 Pursuing M.C.A
QIS COLLEGE OF ENGINEERING & TECHNOLOGY
Vengamukkapalem(V), Ongole, Prakasam dist., Andhra Pradesh- 523272

Abstract: The growth of cyber threats demands a robust and adaptive intrusion detection system (IDS) capable of effectively recognizing malicious activities from network traffic. However, the existing class imbalance in network data presents a significant challenge to traditional IDS. To address this issue, feature selection (FS) techniques are applied, such as recursive feature elimination (RFE) to reduce the dimensionality of the data and enhance the performance of the intrusion detection models. A novel approach is proposed that leverages an ensemble method, integrating the strengths of multiple classifiers to effectively manage class imbalance and improve detection accuracy. The model is evaluated on the CIC-IDS 2017 dataset, which includes a variety of network traffic scenarios and attack patterns. After applying advanced preprocessing and FS techniques, the ensemble model achieves high performance, with the voting classifier (RF + DT) reaching an impressive accuracy of 99.5%. The results demonstrate the effectiveness of the proposed method in handling imbalanced data while maintaining high detection performance, making it a promising solution for enhancing the reliability and efficiency of IDS in real-world cyber defense scenarios.

"Index Terms – *CIS IDS, cyber security, deep learning (DL), ensemble learning, intrusion detection, network security, Voting Classifier ".*

1. INTRODUCTION

In today's digital age, where communication networks underpin the infrastructure of nearly every sector, ensuring the security of these systems has never been more critical. With the increasing frequency and sophistication of cyber-attacks, protecting sensitive data and maintaining operational integrity has become a top priority for organizations worldwide. Among the various types of cyber threats, intrusions in network traffic represent one of the most insidious and challenging risks. These intrusions exploit vulnerabilities in the system, compromising the integrity and security of communication networks. They can go undetected for long periods, making them particularly dangerous and difficult to mitigate. Traditional intrusion detection systems (IDS) primarily rely on rule-based or signature-based methods, which are often limited in their ability to adapt to the evolving landscape of modern cyber threats. Such systems typically use predefined rules or known attack signatures to identify malicious activities. However, they struggle to recognize new, unseen attacks that

deviate from these established patterns, highlighting the need for more adaptive and intelligent IDS solutions [1][2].

The growing complexity and dynamism of cyber threats have driven the demand for advanced IDS that can more effectively identify and qualify emerging threats. Machine learning techniques have emerged as a promising approach to address these limitations, offering the ability to learn from data, adapt to new scenarios, and improve detection accuracy over time [3]. By utilizing machine learning models, IDS can analyze large volumes of network traffic and identify anomalous behavior that could indicate an intrusion. One significant challenge in network traffic analysis is the issue of class imbalance, where the majority of network traffic consists of normal data, with a small fraction representing malicious activities. This imbalance can lead to poor detection rates, especially for rare but critical threats like intrusions. When a network is unbalanced, with some parts seeing much more traffic than others, it creates opportunities for attackers to exploit the less-monitored areas. Similar to how a thief might target a poorly secured neighborhood, cyber attackers can use quieter, less-monitored parts of the network to bypass traditional security measures [4].

Addressing this imbalance is crucial for the effective functioning of intrusion detection systems. Without proper monitoring across the entire network, even areas with low traffic can become vulnerable to attack. Therefore, ensuring that every part of the network is equally monitored and protected, regardless of its activity level, is essential for maintaining robust security. Recent research has shown that advanced machine learning techniques, when combined with novel approaches to class imbalance and feature selection, can significantly enhance IDS performance, making them more resilient to emerging cyber threats [5][6][7]. This new wave of adaptive IDS is not only a solution to the limitations of traditional systems but also a crucial step towards building more secure and resilient network infrastructures.

2. RELATED WORK

Recent advances in intrusion detection systems (IDS), particularly in the domain of machine learning and intelligent systems, have garnered significant attention as cyber-attacks and network intrusions become increasingly sophisticated. These advancements are particularly relevant in the context of sensitive infrastructures, such as unmanned aerial vehicles (UAVs) and transportation networks, where the security of network communications is paramount. The growing complexity of cyber threats has prompted researchers to explore innovative IDS methods that can adapt to new types of attacks and address the challenges posed by class imbalance in network traffic. This literature survey discusses several key contributions to the field, focusing on the role of machine learning in enhancing IDS capabilities and the integration of novel approaches to address the inherent challenges.

Bangui and Buhnova [13] provide an insightful survey of recent developments in machine-learning driven intrusion detection systems (IDS) specifically applied to transportation systems. The authors explore the challenges and solutions related to cybersecurity in transportation, including smart cities, intelligent transportation systems, and UAVs. Their work emphasizes the need for intelligent systems capable of handling large volumes of data generated by these systems. The survey highlights the application of machine learning algorithms, such as decision trees, support vector machines (SVM), and deep learning models, which have shown

promise in identifying anomalous traffic patterns and detecting intrusions in transportation networks. One significant contribution of their work is the emphasis on the need for adaptive systems that can evolve with new attack vectors and rapidly changing network conditions.

In a similar vein, Chen et al. [14] introduce a UAV network intrusion detection method based on spatio-temporal graph convolutional networks (GCN). UAV networks, which are used in various applications such as surveillance, communication, and data collection, are vulnerable to cyber-attacks due to their decentralized and dynamic nature. The authors propose a novel approach using spatio-temporal GCNs to model the spatial and temporal dependencies in network traffic. This method leverages the graph structure of UAV networks, allowing for the detection of complex attack patterns that may not be immediately apparent using traditional methods. The integration of GCNs allows for better generalization and adaptability to changing attack behaviors, making it an important contribution to enhancing the security of UAV networks.

Basan et al. [15] propose an intelligent IDS for a group of UAVs, focusing on securing multi-UAV systems used for collaborative tasks such as reconnaissance and monitoring. The paper highlights the importance of maintaining the integrity and confidentiality of communications within these groups, where each UAV may need to share sensitive information with others. The authors suggest using an intelligent IDS that employs machine learning techniques to detect intrusions and malicious activities, ensuring that the collaborative network of UAVs remains secure. The proposed system is designed to adapt to the dynamic nature of UAV communications, where traffic patterns can change rapidly depending on mission parameters. This adaptability makes the proposed IDS particularly valuable for real-time defense against evolving threats.

Praveena et al. [16] address the problem of intrusion detection in UAVs using deep reinforcement learning (DRL). The authors propose an optimal DRL framework that enhances the IDS by dynamically learning from network traffic and adapting to the changing environment. By incorporating DRL, the system is capable of improving its performance over time, learning to detect intrusions based on feedback from previous actions. The proposed method is particularly effective in situations where UAV networks face novel or unseen threats, as it enables the IDS to continuously refine its detection capabilities. The ability of the DRL model to operate in real-time and adjust its strategies in response to new attack patterns is a significant advantage in the context of UAV security.

Whelan et al. [17] explore the role of artificial intelligence in enhancing IDS for UAV systems. They review various AI techniques, including machine learning, deep learning, and artificial neural networks (ANNs), and their applications in securing UAV networks. The paper highlights the potential of AI-driven approaches to improve the detection and classification of attacks by learning from historical attack data and adapting to new threats. The authors emphasize that traditional signature-based IDS methods are not sufficient for UAVs, as they fail to detect unknown or novel threats. AI models, by contrast, have the potential to provide more accurate and comprehensive detection capabilities. Whelan et al. also discuss the importance of integrating AI techniques with real-time data processing to ensure that intrusion detection is timely and effective.

Abu Al-Haija and Al Badawi [18] focus on the use of deep learning to develop high-performance IDS for networked UAVs. The authors propose a deep learning-based IDS that incorporates convolutional neural networks (CNNs) to extract features from raw network traffic data. The system is designed to handle the unique challenges of UAV networks, such as mobility, dynamic topology, and limited computational resources. The proposed IDS utilizes a deep learning model that is trained on large datasets to detect both known and unknown attacks. The system's ability to generalize from the training data makes it highly effective in detecting a wide range of intrusions, including zero-day attacks. The work of Abu Al-Haija and Al Badawi highlights the importance of deep learning in enhancing the scalability and accuracy of IDS in UAV environments.

Fotohi et al. [19] propose a self-adaptive IDS for securing UAV-to-UAV communications, inspired by the human immune system. The authors present a biologically inspired model that adjusts its detection strategies based on the evolving nature of attacks. The system uses a set of rules that mimic the behavior of the human immune system to recognize and respond to potential intrusions. This adaptive approach allows the IDS to maintain high detection accuracy, even as attackers modify their tactics over time. By simulating the immune response, the system is able to dynamically adjust to new threats, improving its ability to defend against complex and evolving attacks in UAV networks.

He et al. [20] introduce a GAN-based collaborative intrusion detection system for UAV networks, using a blockchain-empowered distributed federated learning approach. The authors combine the generative adversarial network (GAN) with federated learning to create a decentralized system capable of training intrusion detection models across multiple UAVs without sharing sensitive data. This approach addresses concerns related to data privacy and security, as each UAV can independently contribute to the model without exposing its traffic data. The use of GANs in this context allows for the generation of synthetic data to augment training datasets, improving the model's ability to detect rare or novel attacks. The integration of blockchain further enhances the system's security by ensuring the integrity of the detection process.

These studies collectively highlight the significant advances in IDS for UAV and transportation networks, with a strong focus on machine learning and deep learning techniques. The integration of advanced algorithms, such as deep reinforcement learning, graph convolutional networks, and GANs, provides a robust framework for addressing the dynamic and evolving nature of cyber threats. Additionally, the use of adaptive and biologically inspired models, such as the immune system-based IDS, demonstrates the potential for developing IDS systems that can respond intelligently to new attack patterns. As UAV networks and other critical infrastructures continue to expand, these innovative approaches will be crucial in ensuring the security and reliability of networked systems.

3. MATERIALS AND METHODS

The proposed system aims to address the challenges of class imbalance and improve the performance of Intrusion Detection Systems (IDS) by leveraging a combination of advanced feature selection (FS) techniques and ensemble learning. To handle high-dimensional network traffic data, FS techniques such as Recursive Feature Elimination (RFE) will be applied to reduce the feature space while retaining the most relevant information. The ensemble method integrates multiple classifiers, including

XGBoost [8], LSTM [9], minVGG [12] (1D CNN), AlexNet (1D CNN), and CNN + BiLSTM [10], to enhance detection accuracy and robustness. Each model brings a unique strength to the table: XGBoost for its gradient boosting capabilities, LSTM for sequential data analysis, CNN-based models (minVGG and AlexNet) for feature extraction, and BiLSTM for capturing both forward and backward temporal dependencies. The ensemble approach, particularly through the Voting Classifier combining Random Forest (RF) and Decision Tree (DT), will help mitigate class imbalance, making the system more adaptable and effective in real-world cyber defense scenarios. The system will be evaluated on the CIC-IDS 2017 dataset [11] to assess its performance in detecting diverse attack patterns.

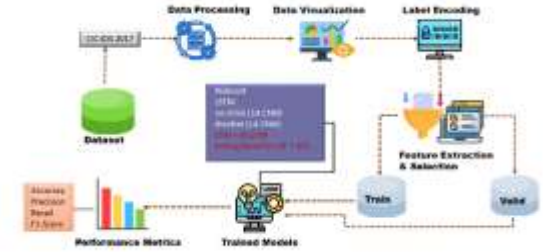


Fig.1 Proposed Architecture

The architecture uses the CIC-IDS 2017 dataset [11] for data processing and visualization. After label encoding, feature extraction and selection are performed. The dataset is then split into train and valid sets. Multiple models like XGBoost [8], LSTM [9], miniVGG, AlexNet [12], 3dCNN, CNN+BLSTM [10], and Voting Classifier are trained and evaluated on the dataset. Performance metrics like accuracy, precision, recall, and F1-score are used to assess the models.

i) Dataset Collection:

The dataset used for this study is the CIC IDS 2017 [11], which contains network traffic data for intrusion detection, specifically focusing on the analysis of packet-level features. Initially, the dataset comprises 78 attributes across 17,697 entries, representing various network traffic metrics. After performing feature selection, a subset of 10 key features was identified, which includes 'Bwd Packet Length Mean', 'Bwd Packet Length Std', 'Fwd IAT Total', 'Fwd IAT Mean', 'Fwd IAT Min', 'Bwd IAT Std', 'Bwd Packets/s', 'Avg Packet Size', 'Avg Bwd Segment Size', and 'Subflow Bwd Packets'. These features capture critical aspects of network flow, such as packet lengths, inter-arrival times, and flow statistics, which are essential for effective intrusion detection. The reduced feature set is utilized for model training to improve the accuracy and efficiency of the detection system.

	Protocol	Flow Duration	Total Fwd Packets	Total Backward Packets	Fwd Packets Length Total	Bwd Packets Length Total	Fwd Packet Length Max	Fwd Packet Length Min	Fwd Packet Length Mean
0	6	4	2	0	12	0	6	6	6.00000
1	6	1	2	0	12	0	6	6	6.00000
2	6	3	2	0	12	0	6	6	6.00000
3	6	1	2	0	12	0	6	6	6.00000
4	6	609	7	4	484	414	233	0	69.14286

5 rows × 78 columns

Fig.2 Dataset Collection Table - CIC-IDS 2017

ii) Pre-Processing:

In the pre-processing step, we focus on preparing the dataset for modeling. This includes cleaning the data, visualizing key relationships, encoding categorical labels, and performing feature extraction to ensure high-quality input for the prediction model.

a) Data Processing: The data processing steps involve addressing missing values and duplicate entries to ensure clean and reliable data. First, any rows with missing values are removed to maintain data integrity. Next, duplicate records are identified

and eliminated to avoid redundancy, ensuring that each entry is unique. After these operations, the dataset's index is reset for proper alignment. Additionally, the categorical columns are inspected for further analysis, and the first few rows of the cleaned data are displayed to verify the changes.

b) Data Visualization: Data visualization involves two key analyses. First, a count plot is used to display the distribution of the target variable, highlighting the frequency of each class label in the dataset. This helps in understanding the balance or imbalance between different categories. Second, a heatmap is generated to visualize the correlation matrix of the dataset. The heatmap highlights the relationships between various features, with color intensity indicating the strength of correlations, allowing for easy identification of strongly correlated variables.

c) Label Encoding: Label encoding is a technique used to convert categorical labels into numerical values. In this case, the target variable, 'Label', is transformed by assigning each unique category a distinct integer value. This process is particularly useful for machine learning models, as they require numerical input. After encoding, each label is represented by a unique number, making the dataset more suitable for modeling while maintaining the integrity of the original categorical information. The transformed labels are then ready for further analysis or training.

d) Feature Extraction: Feature extraction involves identifying and defining key variables that represent the input for the model. The dataset is divided into features (X) and the target variable (y). The features include all columns except the 'Label' column, which is designated as the target. This step ensures that the dataset is properly structured for further analysis. The features capture relevant characteristics of the network traffic, forming the foundation for the detection process.

e) Feature Selection: Feature selection refines the dataset by identifying the most significant variables to improve model performance. Recursive Feature Elimination (RFE) is applied to iteratively evaluate and remove less important features, retaining only the most impactful ones. In this case, 10 key features are selected to optimize predictions: Flow Duration, Total Fwd Packets, Total Length of Fwd Packets, Flow Bytes/s, Flow Packets/s, Fwd Packet Length Mean, Bwd Packet Length Mean, Average Packet Size, Packet Length Std, and FIN Flag Count. These features are critical for accurately identifying and classifying network traffic, ensuring the model's efficiency and effectiveness.

iii) Training & Testing:

In the training and testing process, the dataset is divided into two parts: one for training the model and the other for testing its performance. The training data is used to teach the model how to predict the target variable, while the testing data is kept aside to evaluate the model's ability to make predictions on unseen data. This approach helps in assessing the model's generalization ability and ensures that it performs well on new, unseen data, preventing overfitting.

iv) Algorithms:

XGBoost: This algorithm is utilized to enhance predictive accuracy by handling large datasets and complex relationships. Its [8] boosting technique ensures better performance by sequentially correcting errors made by previous models, making it ideal for classification tasks with high-dimensional data.

LSTM: Long Short-Term Memory is applied for modeling sequential data by capturing long-term dependencies. It [9] excels in scenarios where past observations influence future predictions, making it particularly effective for tasks involving time-series data or sequences, such as forecasting.

minVGG (1d CNN): This model [12] is used for extracting spatial features from sequential or time-series data. By using 1D convolutions, it helps in identifying local patterns, making it well-suited for classification tasks where temporal or sequential features are crucial for accuracy.

AlexNet (1d CNN): AlexNet is implemented to learn deep features from sequential data through 1D convolutions. It [12] enhances the extraction of complex patterns from input data, allowing for improved recognition and classification, especially in cases where the data's spatial hierarchy is significant.

CNN + BiLSTM: This combined architecture leverages both convolutional layers and bidirectional LSTMs to extract spatial and temporal features. It [10] is highly effective in tasks that require understanding both the local patterns and the sequence context, improving performance in complex data classification.

Voting Classifier (RF + DT): This ensemble model integrates predictions from Random Forest and Decision Tree classifiers. By combining their strengths, it boosts overall accuracy and robustness, ensuring that the final prediction is more reliable and less prone to errors compared to individual models.

4. RESULTS & DISCUSSION

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} \ + \ \mathrm{FN}} (3)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

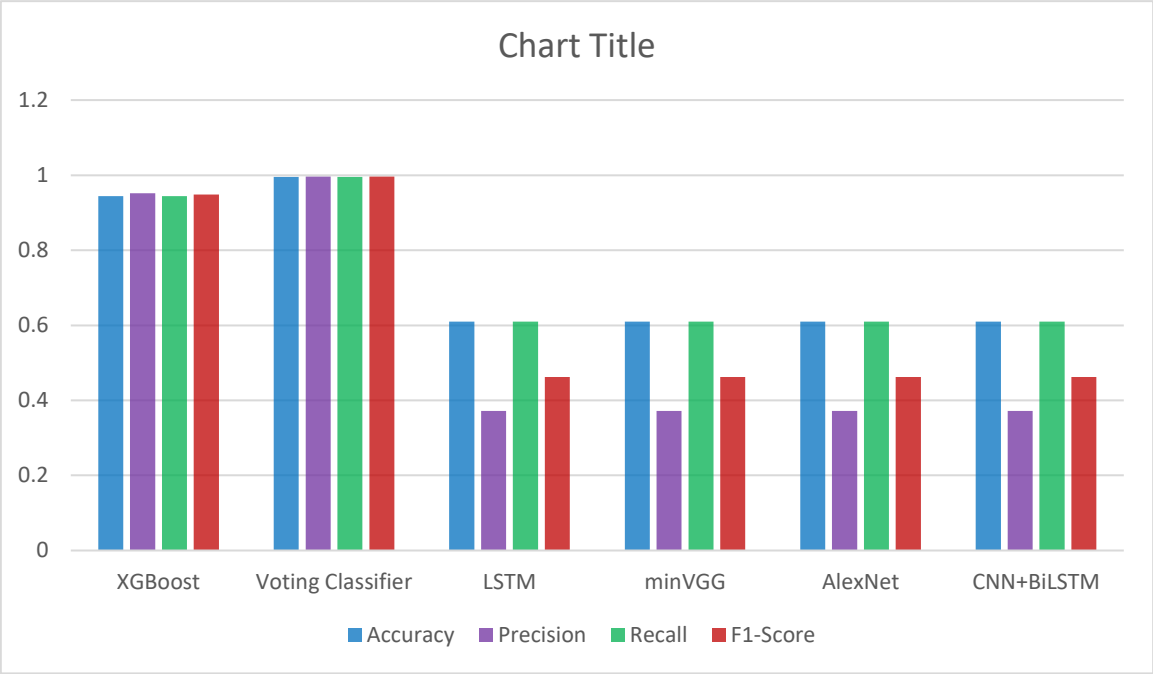
$$F1\ Score = 2 * \frac{Recall\ \mathrm{X}\ Precision}{Recall + Precision} * 100 (1)$$

Table (1) evaluate the performance metrics — accuracy, precision, recall and F1-Score—for each algorithm. Across all metrics, the Voting Classifier consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

Table.1 Performance Evaluation Metrics

Model	Accuracy	Precision	Recall	F1-Score
XGBoost	0.944	0.952	0.944	0.948
Voting Classifier	**0.995**	**0.996**	**0.995**	**0.996**
LSTM	0.610	0.372	0.610	0.462
minVGG	0.610	0.372	0.610	0.462
AlexNet	0.610	0.372	0.610	0.462
CNN+BiLSTM	0.610	0.372	0.610	0.462

Graph.1 Comparison Graphs



Accuracy is represented in blue, precision in purple, recall in green, and F1-Score in red, ***Graph (1)***. In comparison to the other models, the Voting Classifier shows superior performance across all metrics, achieving the highest values. The graphs above visually illustrate these findings.

Fig. 3 Dash Board

The Fig. 3 shows the user dashboard of an intrusion detection system (IDS). It has a welcoming message and an illustration of people working on computers. There is also a "Signup" button and a "Read More" link.

Step - 7

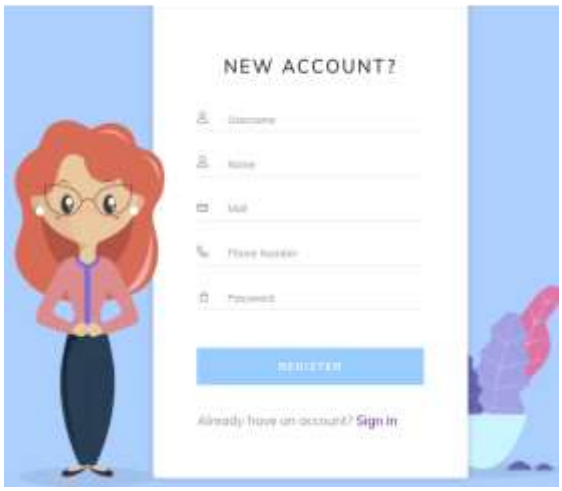


Fig. 4 Register page

The Fig. 4 shows a user registration form with a cartoon illustration. It asks for a username, name, email, phone number, and password. There is also a "REGISTER" button and a link to "Sign in" for existing users.

Step - 8

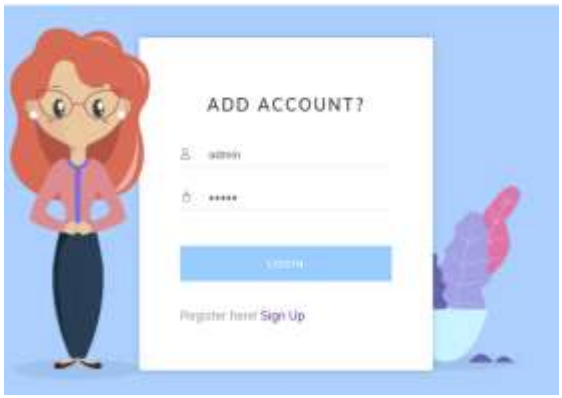


Fig. 5 Login page

The Fig. 5 shows a login page with a cartoon character. It asks for a username and password. There is also a "LOGIN" button and a link to "Sign Up" for new users.

Step - 9

Fig. 6 Home page

The Fig. 6 shows the main page of a dashboard with the title "WELCOME TO DASHBOARD." There are tabs for "Prediction," "Graph," "Notebook," and "Signout." The background image depicts people working with data, suggesting the dashboard is used for data analysis and visualization.

Step – 10
Test case 1

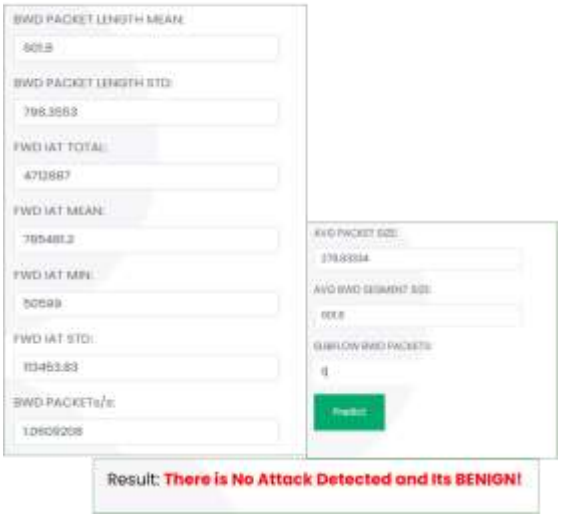


Fig. 7 Test case – 1

The Fig. 7 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts

the outcome as "BENIGN," indicating no attack detected.

Fig. 8 Test case – 2

The Fig. 8 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts the outcome as a "BOT ATTACK."

Fig. 9 Test case – 3

The Fig. 9 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts the outcome as a "BRUTEFORCE ATTACK."

Fig. 10 Test case – 4

The Fig. 10 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts the outcome as a "DDOS ATTACK."

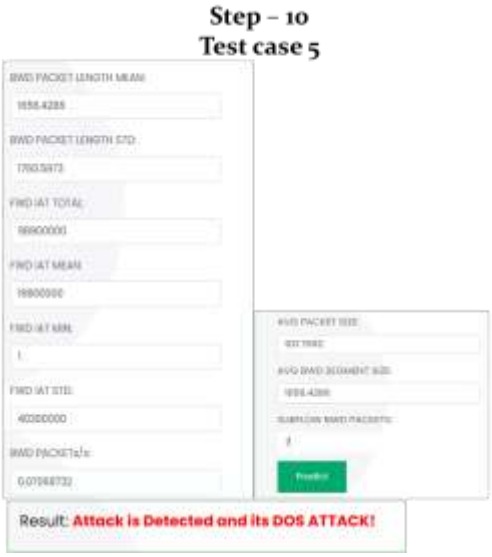


Fig. 11 Test case – 5

The Fig. 11 shows a network intrusion detection system. It collects data like packet lengths, intervals,

and rates. After inputting data, the system predicts the outcome as a "DOS ATTACK."

Fig. 12 Test case – 6

The Fig. 12 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts the outcome as a "PORTSCAN ATTACK."

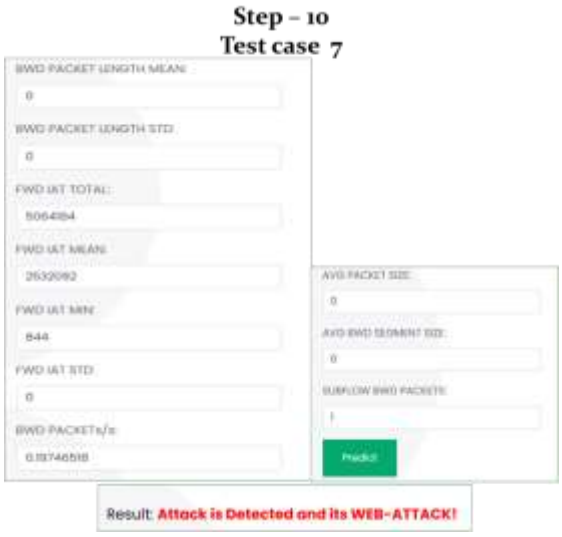


Fig. 13 Test case – 7

The Fig. 13 shows a network intrusion detection system. It collects data like packet lengths, intervals, and rates. After inputting data, the system predicts the outcome as a "WEB-ATTACK."

5. CONCLUSION

In conclusion, the proposed approach demonstrates the effectiveness of using advanced feature selection techniques and an ensemble model to tackle the class imbalance issue in network intrusion detection. By leveraging the strengths of multiple classifiers, the ensemble method significantly enhances detection accuracy. The model was evaluated on the CIC-IDS 2017 dataset, which covers various network traffic scenarios and attack patterns. Among the tested models, the voting classifier stood out with an impressive accuracy of 99.5%. This high-performance result confirms the ability of the proposed solution to accurately detect intrusions despite the challenges posed by imbalanced data. The approach successfully addresses the limitations of traditional IDS models, providing a robust and reliable solution for real-world cyber defense applications.

Future work could focus on enhancing the ensemble model by integrating more advanced algorithms, such as deep learning techniques, to further improve detection accuracy and adaptability. Additionally, exploring the use of real-time data streams for dynamic intrusion detection could help adapt the system to evolving cyber threats. Other potential directions include incorporating additional network traffic features and investigating domain-specific optimizations for specific types of attacks, thereby refining the model's performance in diverse network environments and enhancing its overall robustness.

REFERENCES

[1] R. R. Kumar, A. Tomar, M. Shameem, and M. N. Alam, ‘‘OPTCLOUD: An optimal cloud service

selection framework using QoS correlation lens,'' Comput. Intell. Neurosci., vol. 2022, pp. 1–16, May 2022, doi: 10.1155/2022/2019485.

[2] R. R. Kumar, M. Shameem, and C. Kumar, ''A computational frame work for ranking prediction of cloud services under fuzzy environment,'' Enterprise Inf. Syst., vol. 16, no. 1, pp. 167–187, Jan. 2022, doi: 10.1080/17517575.2021.1889037.

[3] M. A. Akbar, M. Shameem, S. Mahmood, A. Alsanad, and A. Gumaei, ''Prioritization based taxonomy of cloud-based outsource software devel opment challenges: Fuzzy AHP analysis,'' Appl. Soft Comput., vol. 95, Oct. 2020, Art. no. 106557, doi: 10.1016/j.asoc.2020.106557.

[4] M.Bakro, S.K.Bisoy, A.K.Patel, and M.A.Naal, ''Performance analysis of cloud computing encryption algorithms,'' in Advances in Intelligent Computing and Communication, vol. 202. Cham, Switzerland: Springer, 2021, pp. 357–367.

[5] (2030). Cyber Security Market Share, Forecast | Growth Analysis. Accessed: Apr. 23, 2023. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/cyber-securitymarket-101165Benamor

[6] S. Lipsa and R. K. Dash, ''A novel dimensionality reduction strategy based on linear regression with a fine-pruned decision tree classifier for detecting DDoS attacks in cloud computing environments,'' in Proc. 1st Int. Symp. Artif. Intell., 2022, pp. 15–25.

[7] X. Tan, S. Su, Z. Zuo, X. Guo, and X. Sun, ''Intrusion detection of UAVs based on the deep belief network optimized by PSO,'' Sensors, vol. 19, no. 24, p. 5529, Dec. 2019.

[8] Attia, A., Faezipour, M., & Abuzneid, A. (2020, December). Network intrusion detection with XGBoost and deep learning algorithms: an evaluation study. In 2020 international conference on computational science and computational intelligence (CSCI) (pp. 138-143). IEEE.

[9] Boukhalfa, A., Abdellaoui, A., Hmina, N., & Chaoui, H. (2020). LSTM deep learning method for network intrusion detection system. International Journal of Electrical and Computer Engineering, 10(3), 3315.

[10] P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Hao, and J. Chen, "Dlids: Extracting features using cnn-lstm hybrid network for intrusion detection system," Security and Communication Networks, 2020.

[11] R. Panigrahi and S. Borah, "A detailed analysis of CIC IDS 2017 dataset for designing intrusion detection systems," International Journal of Engineering & Technology, vol. 7, no. 3.24, pp. 479–482, 2018.

[12] Zhang, X., Chen, J., Zhou, Y., Han, L., & Lin, J. (2019). A multiple-layer representation learning model for network-based attack detection. IEEE Access, 7, 91992-92008.

[13] H. Bangui and B. Buhnova, ''Recent advances in machine-learning driven intrusion detection in transportation: Survey,'' Proc. Comput. Sci., vol. 184, pp. 877–886, Aug. 2021.

[14] Z.Chen, N.Lyu, K.Chen, Y.Zhang, and, W.Gao, ''UAV network intrusion detection method based on spatio-temporal graph convolutional network,'' J. Beijing Univ. Aeronaut. Astronaut., vol. 47, no. 5, pp. 1068–1076, 2021.

[15] E. Basan, M. Lapina, N. Mudruk, and E. Abramov, ''Intelligent intrusion detection system

for a group of UAVs,'' in Proc.12th Int.Conf.Adv.Swarm Intell., 2021, pp. 230–240.

[16] V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea, S. Y. Alyahyan, and M. A. Raza, ''Optimal deep reinforcement learning for intrusion detection in UAVs,'' Comput., Mater. Continua, vol. 70, no. 2, pp. 2639–2653, 2022.

[17] J. Whelan, A. Almehmadi, and K. El-Khatib, ''Artificial intelligence for intrusion detection systems in unmanned aerial vehicles,'' Comput. Electr. Eng., vol. 99, Apr. 2022, Art. no. 107784.

[18] Q. Abu Al-Haija and A. Al Badawi, ''High-performance intrusion detection system for networked UAVs via deep learning,'' Neural Comput.Appl., vol. 34, no. 13, pp. 10885–10900, Jul. 2022.

[19] R.Fotohi, M. Abdan,andS.Ghasemi,''A self-adaptive intrusion detection system for securing UAV-to-UAV communications based on the human immune system in UAV networks,'' J. Grid Comput., vol. 20, no. 3, p. 22, Sep. 2022.

[20] X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, ''CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach,'' IEEE Internet Things J., vol. 10, no. 1, pp. 120–132, Jan. 2023.

AUTHORS

Mr. K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.