iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80148

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Smart Shield: Machine Learning-Based Intrusion Detection System

Sabavath Raju[1], T. Saisree[2], V. Praveen[3], P. Ajay[4], G. Harish[5]
Computer Science and Engineering (Cyber Security), Pallavi Engineering College, Hyderabad

Abstract: ***With the rapid growth of networked systems and internet-based services, cybersecurity has become a critical concern for organisations and individuals. Intrusion Detection Systems (IDS) play a vital role in identifying malicious activities and protecting network infrastructure from potential threats. This paper presents a machine learning-based approach for detecting network intrusions using the dataset. The proposed system involves data preprocessing, feature selection, and the application of classification algorithms to accurately distinguish between normal and attack traffic. Various machine learning models are implemented and evaluated based on performance metrics such as accuracy, precision, recall, and F1-score. The experimental results demonstrate that the proposed approach effectively identifies different categories of attacks, including DoS, Probe, R2L, and U2R, while reducing false alarm rates. The model shows improved detection capability compared to traditional rule-based systems, making it suitable for real-world cybersecurity applications. This study highlights the potential of machine learning techniques in enhancing intrusion detection mechanisms and provides a foundation for developing more advanced and adaptive security solutions. This project, Smart Shield: ML-Based Intrusion Detection System, uses machine learning algorithms to detect network intrusions and classify traffic as normal or malicious. The system uses publicly available datasets such as UNSW-NB15, NetFlow, NSL-KDD and CIC-IDS datasets to train the detection model. The system employs algorithms like Random Forest and Decision Tree to analyse network features and detect suspicious patterns. The developed system processes network traffic data, performs feature extraction and preprocessing, and uses trained machine learning models to detect attacks.***

Keywords: Intrusion Detection System, Machine Learning, Network Security, Cyber Security, Classification Algorithms.

I. INTRODUCTION

In the contemporary digital landscape, the exponential growth of networked systems, cloud platforms, and internet-driven applications has significantly increased exposure to cyber threats, making network security a critical concern for organisations and individuals alike. As cyberattacks become more sophisticated, traditional security mechanisms such as firewalls and encryption alone are no longer sufficient to ensure complete protection, as they primarily focus on prevention rather than detection of ongoing or unknown attacks. This has led to the growing importance of Intrusion Detection Systems (IDS), which continuously monitor network traffic to identify suspicious activities and potential security breaches. IDS can be categorised into signature-based and anomaly-based approaches; however, conventional systems often struggle with limitations such as high false alarm rates, inability to detect zero-day attacks, and poor adaptability to evolving attack patterns. To overcome these challenges, machine learning techniques have emerged as a powerful solution due to their ability to learn from large volumes of data, recognise complex patterns, and generalise to previously unseen threats. In this study, a machine learning-based intrusion detection framework is developed by leveraging multiple benchmark datasets, including NSL-KDD, NetFlow, UNSW-NB15, and CIC-IDS, to ensure a comprehensive evaluation across diverse network traffic scenarios and attack types. Each dataset contributes unique characteristics: NSL-KDD provides a refined version of traditional intrusion data, UNSW-NB15 includes modern synthetic attack behaviours, CIC-IDS offers realistic traffic patterns with up-to-date attack representations, and NetFlow data captures flow-based network features widely used in real-time monitoring systems. By integrating these diverse datasets, the proposed system aims to enhance detection robustness, reduce bias, and improve generalisation across different network environments. The methodology involves data preprocessing, feature engineering, and the application of various machine learning algorithms to classify network traffic into normal and malicious categories, including attacks such as denial-of-service (DoS), probing, remote-to-local (R2L), and user-to-root (U2R), along with other contemporary threats.

II. LITERATURE REVIEW

Several research works have been conducted in the field of intrusion detection systems using machine learning [12][13]. Many traditional IDS systems use signature-based detection techniques, which depend on known attack patterns [4][5]. These systems fail to detect new or unknown attacks [12].

Researchers have proposed machine learning-based IDS models that analyse network traffic patterns and automatically detect anomalies [2][3]. Algorithms such as Decision Tree, Random Forest, Support Vector Machine, and Neural Networks have been widely used for intrusion detection [1][2][14]. Studies have shown that Random Forest algorithms provide higher accuracy and better performance in detecting attacks compared to other models [11][13]. Random Forest uses multiple decision trees to improve prediction accuracy and reduce overfitting [11].

Datasets such as KDD Cup 99, NSL-KDD, and UNSW-NB15 are commonly used for evaluating IDS systems [6][7][8]. These datasets contain various types of network attacks, including DoS, Probe, and malware traffic [7][8]. However, many existing IDS solutions still face challenges such as high false positives and limited scalability [12]. While many approaches have achieved promising results, challenges such as dataset imbalance, high computational complexity, and lack of generalisation across different network environments persist [12][13]. Recent works emphasise the importance of hybrid models and multi-dataset approaches to overcome these limitations [13].

III. PROPOSED SYSTEM

To overcome the limitations of traditional intrusion detection approaches, this paper proposes a robust and scalable machine learning-based Intrusion Detection System (IDS) that leverages multiple benchmark datasets, including NSL-KDD, NetFlow, UNSW-NB15, and CIC-IDS. The proposed system is designed to enhance detection accuracy, improve generalisation, and effectively identify both known and unknown cyber threats across diverse network environments. By integrating multiple datasets, the system captures a wide range of traffic patterns and attack behaviours, thereby reducing dataset bias and enabling the model to perform reliably in real-world scenarios. The architecture of the proposed system consists of several key stages, including data collection, preprocessing, feature engineering, model training, and evaluation. Initially, data from the four datasets is consolidated and pre-processed to handle missing values, remove redundant features, and normalise the data for consistency. Feature selection techniques are applied to identify the most relevant attributes, reducing dimensionality and improving model performance. The processed data is then used to train various machine learning classification algorithms such as XG-Boost, Random Forest, Support Vector Machine, and K-Nearest Neighbours, which are capable of learning complex patterns and distinguishing between normal and malicious traffic. The system classifies network traffic into multiple categories, including normal activity and different types of attacks such as Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R), along with modern attack types present in UNSW-NB15 and CIC-IDS datasets. Performance evaluation is carried out using metrics such as accuracy, precision, recall, and F1-score to ensure a comprehensive assessment of the model's effectiveness.

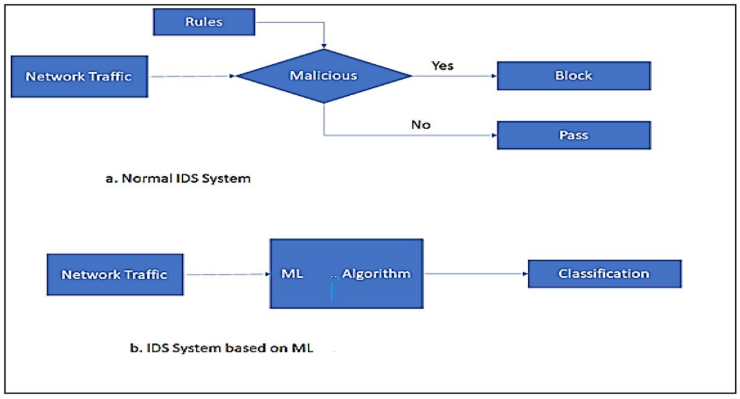


Fig 1 Normal IDS System VS Machine Learning-Based IDS System

IV. EXPERIMENTAL RESULTS

The experimental evaluation of the proposed Intrusion Detection System (IDS) was conducted using four benchmark datasets: NSL-KDD, NetFlow, UNSW-NB15, and CIC-IDS, to ensure a comprehensive assessment across diverse network traffic scenarios. The datasets were pre-processed and divided into training and testing sets to evaluate the performance of the selected machine learning algorithms-XG-Boost, Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbours (KNN). The models were assessed using standard evaluation metrics such as accuracy, precision, recall, and F1-score. The results indicate that XG-Boost achieved the highest performance among all models, demonstrating superior capability in handling complex and high-dimensional data.

Random Forest also performed consistently well, providing high accuracy and stability across all datasets. SVM showed reliable classification performance with balanced precision and recall, while KNN exhibited comparatively lower accuracy due to its sensitivity to large-scale data and computational complexity. The use of multiple datasets significantly improved the generalisation ability of the models and reduced bias associated with single-dataset training. Overall, the experimental results confirm that the proposed system is effective in accurately detecting various types of network intrusions with reduced false positives, making it suitable for real-time cybersecurity applications.

A. The detailed performance metrics of the implemented models are shown in Table 1.

TABLE 1
EVALUATION METRICS OF ML MODELS FOR IDS

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
XG-Boost	97	96	95	95.5
Random Forest	96	95	94	94.5
SVM	94	93	92	92.5
KNN	91	90	89	89.5

B. Machine Learning-Based Intrusion Detection System Interface

The figure 2 illustrates the user interface of the proposed Machine Learning-Based Intrusion Detection System (IDS), developed to provide real-time monitoring and analysis of network traffic. The dashboard presents a visually interactive environment that highlights the core functionalities of the system, including the integration of multiple machine learning algorithms such as XG-Boost, Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbours (KNN).

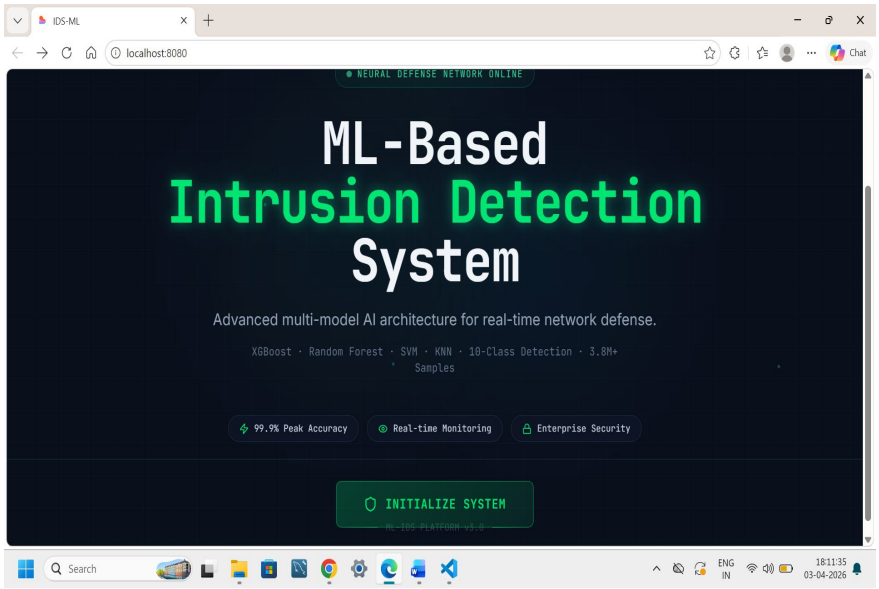


Fig 2 Main Interface of IDS System

C. Model Performance Visualisation Dashboards

The figure presents the dynamic visualisation module of the proposed Machine Learning-Based Intrusion Detection System (IDS), highlighting real-time analysis of network traffic patterns. The dashboard displays a comprehensive technical report interface, including an executive summary and machine learning implementation details. A line/area chart is used to visualise continuous data trends, comparing malicious (threat) and normal network traffic over time.

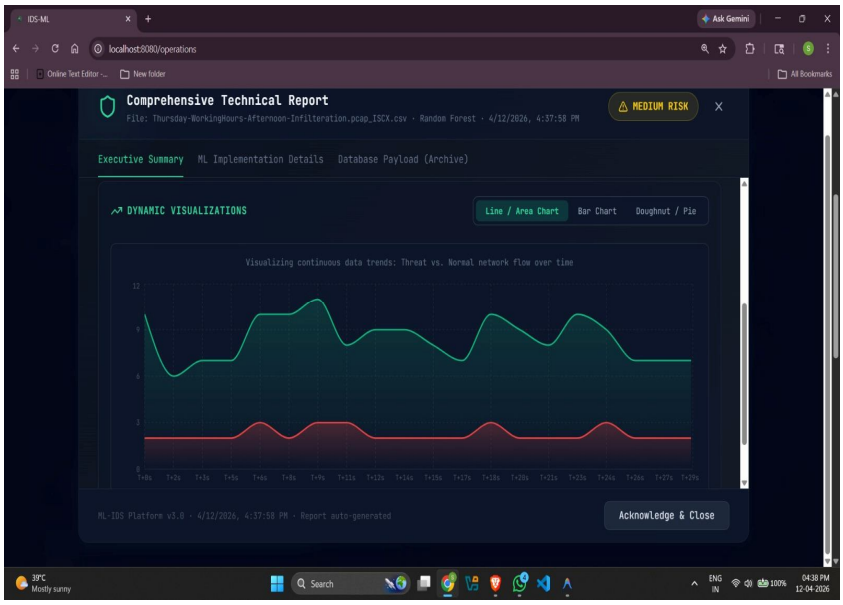


Fig 3 Dynamic Visualisation dashboard showing Threat VS Normal Traffic

The figure illustrates the doughnut chart visualisation module of the proposed Machine Learning-Based Intrusion Detection System (IDS), which provides a proportional representation of different types of detected cyber-attacks. The chart displays the distribution of attack categories, such as exploits, backdoor attacks, and fuzzers, relative to the total number of detected threats. This visual representation enables quick understanding of the dominance and frequency of specific attack types within the analysed network traffic.

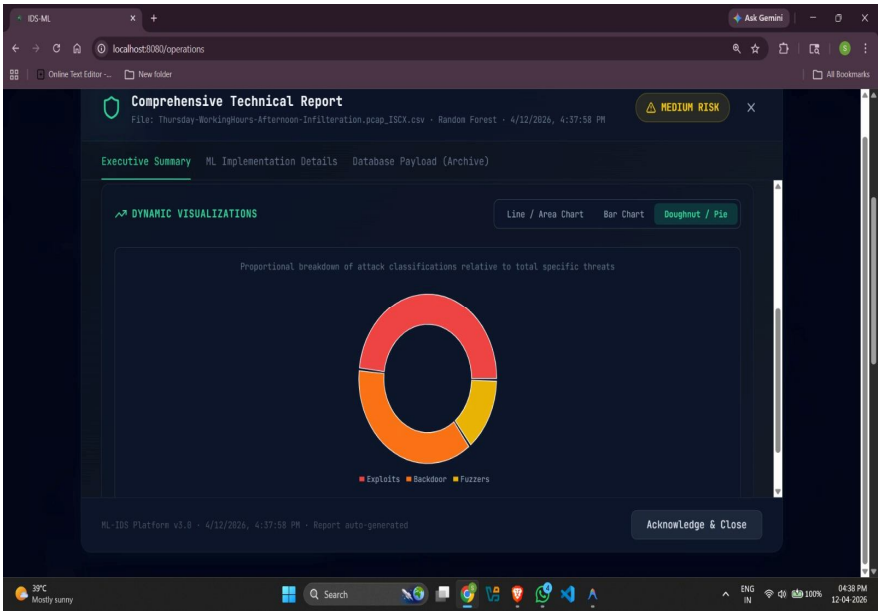


Fig 4 Doughnut Chart Visualization of Attack Classification Distribution

The figure depicts the bar chart visualization module of the proposed Machine Learning-Based Intrusion Detection System (IDS), which presents a comparative analysis of different attack categories detected in network traffic. The chart illustrates the volume of specific attack types such as exploits, backdoor attacks, and fuzzers, enabling clear differentiation based on their frequency of occurrence. This discrete representation allows users to quickly identify which type of attack is most prevalent within the analysed dataset.

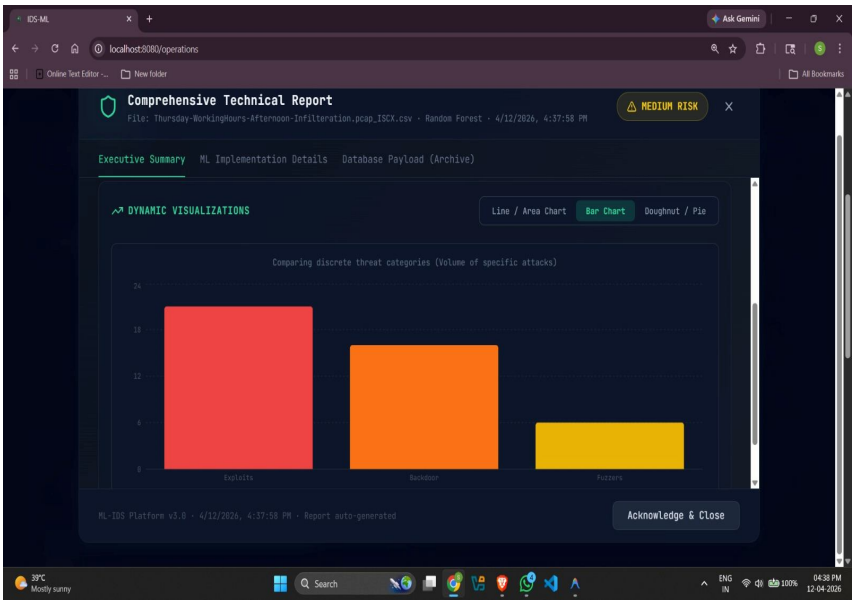


Fig 5 Bar Chart Visualisation of Attack Category Comparison

V. DISCUSSION

The experimental findings highlight the effectiveness of the proposed machine learning-based Intrusion Detection System (IDS) in handling diverse and complex network traffic scenarios. By incorporating multiple datasets such as NSL-KDD, NetFlow, UNSW-NB15, and CIC-IDS, the system overcomes the limitations associated with single-dataset approaches and achieves improved robustness and generalisation. The performance comparison indicates that ensemble-based methods like XG-Boost and Random Forest outperform other algorithms due to their ability to manage high-dimensional data, reduce overfitting, and capture non-linear relationships within network traffic features. Support Vector Machine (SVM) demonstrates consistent and balanced performance across different metrics, while K-Nearest Neighbours (KNN) is relatively less efficient for large-scale data due to its higher computational cost during prediction.

The integration of multiple datasets also enables the system to detect both traditional and modern attack types, making it more suitable for real-world applications. Furthermore, the use of comprehensive evaluation metrics such as accuracy, precision, recall, and F1-score ensures a thorough assessment of the model's performance, particularly in handling imbalanced data and minimizing false positives and false negatives. The visualization components, including line charts, bar charts, and doughnut charts, play a crucial role in enhancing the interpretability of results by providing clear insights into traffic patterns, attack distribution, and temporal variations in network activity. The inclusion of a risk-level indicator further strengthens the system by enabling quick assessment of threat severity, thereby assisting network administrators in timely decision-making.

However, despite the promising outcomes, certain challenges remain. The integration of multiple large datasets increases computational complexity and processing time, which may impact real-time deployment in resource-constrained environments. Additionally, some attack categories with fewer samples may still be difficult to classify accurately due to data imbalance. Future improvements can focus on optimizing model performance through feature selection techniques, balancing datasets, and incorporating deep learning approaches for enhanced detection capabilities. Overall, the proposed system demonstrates significant potential as a scalable, adaptive, and efficient solution for modern intrusion detection, capable of addressing the evolving landscape of cybersecurity threats.

VI. CONCLUSION

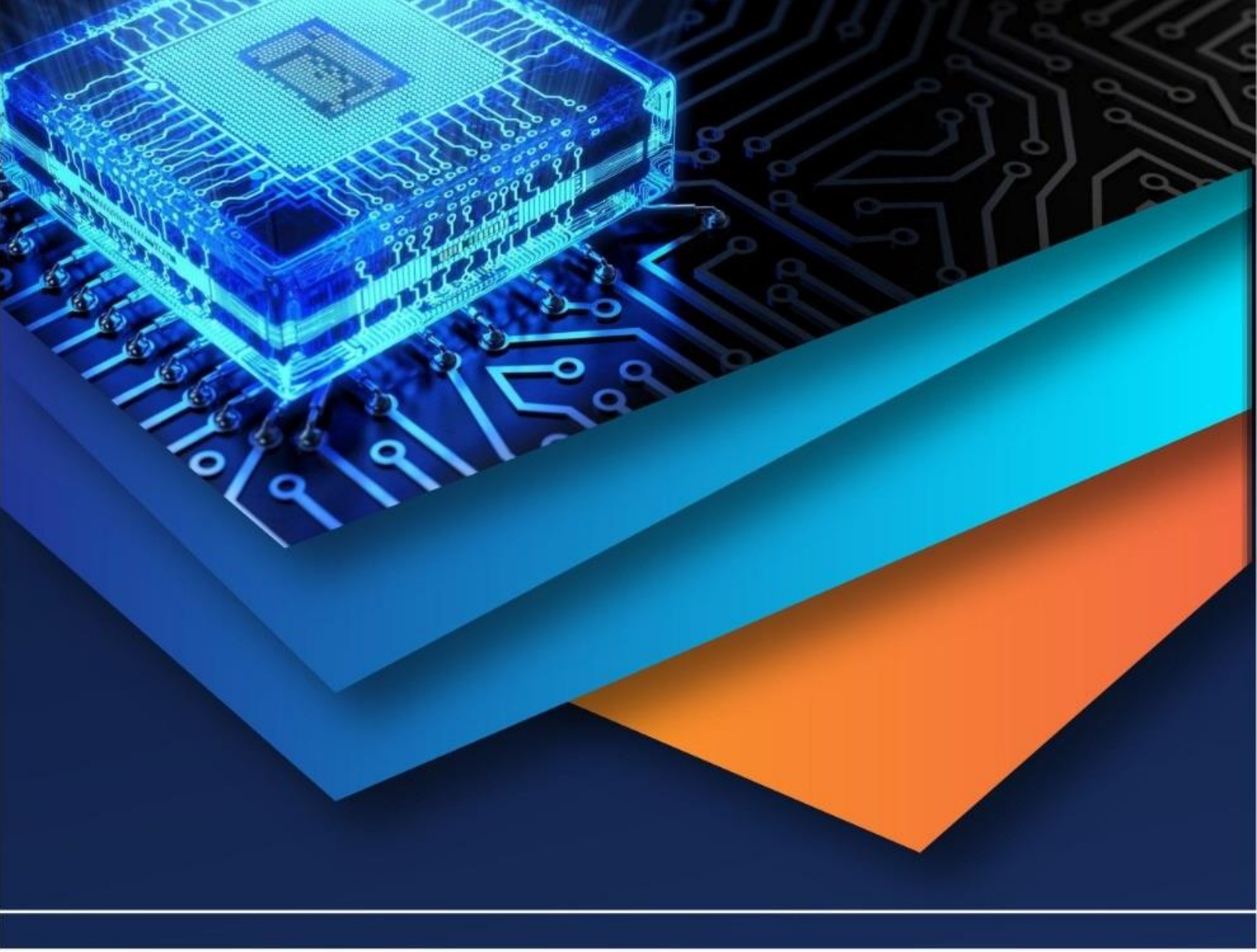
This study presented a comprehensive machine learning-based Intrusion Detection System (IDS) designed to enhance network security by accurately identifying and classifying cyber threats. By leveraging multiple benchmark datasets—NSL-KDD, NetFlow, UNSW-NB15, and CIC-IDS-the proposed system overcomes the limitations of traditional single-dataset approaches and achieves improved robustness and generalisation across diverse network environments. The integration of advanced machine learning algorithms such as XG-Boost, Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbours (KNN) enable effective detection of both known and emerging attack patterns.

The experimental results demonstrate that ensemble methods, particularly XG-Boost and Random Forest, provide superior performance in terms of accuracy, precision, recall, and F1-score, while SVM offers stable and consistent classification results. The system also benefits from comprehensive preprocessing and feature selection techniques, which enhance model efficiency and reduce computational overhead. Additionally, the inclusion of dynamic visualisation modules-such as line charts, bar charts, and doughnut charts-improves the interpretability of results, allowing users to easily analyse network behaviour and attack distributions. The incorporation of a risk-level indicator further supports real-time decision-making and threat assessment.

Despite achieving high performance, certain challenges, such as computational complexity, dataset imbalance, and scalability in real-time environments, remain. These limitations provide opportunities for future enhancement through optimisation techniques, integration of deep learning models, and deployment in real-time network monitoring systems. Overall, the proposed IDS demonstrates strong potential as a scalable, adaptive, and efficient solution for modern cybersecurity challenges, contributing to the development of more intelligent and reliable intrusion detection mechanisms.

REFERENCES

[1] Goodfellow, Ian. "Deep learning." (2016).
[2] Christopher, M. Bishop. "Pattern recognition and machine learning." (2006).
[3] Mitchell, T. M. "'Machine Learning', New York, NY, USA: McGraw-Hill, Inc." (1997).
[4] Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2003.
[5] Forouzan, Behrouz A. Data communications and networking. Huga Media, 2007.
[6] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." 2015 military communications and information systems conference (MilCIS). Ieee, 2015.
[7] Tavallaee, Mahbod, et al. "A detailed analysis of the KDD CUP 99 data set." 2009 IEEE symposium on computational intelligence for security and defense applications. Ieee, 2009.
[8] Lippmann, Richard P., et al. "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation." Proceedings DARPA Information survivability conference and exposition. DISCEX'00. Vol. 2. IEEE, 2000.
[9] Pedregosa, Fabian, et al. "Scikit-learn: Machine learning in Python." the Journal of machine Learning research 12 (2011): 2825-2830.
[10] Sharma, Saurabh & Sharma, Neha & Yadav, Narendra. (2021). Classification of UNSW-NB15 dataset using Exploratory Data Analysis using Ensemble Learning. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems. 8. 171319. 10.4108/eai.13-10-2021.171319.
[11] Mining, What Is Data. "Data mining: Concepts and techniques." Morgan Kaufinann 10.559-569 (2006): 4.
[12] Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer networks 51.12 (2007): 3448-3470.
[13] Folino, Gianluigi, Clara Pizzuti, and Giandomenico Spezzano. "GP ensemble for distributed intrusion detection systems." International Conference on Pattern Recognition and Image Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.
[14] Mukkamala, Srinivas, Guadalupe Janoski, and Andrew Sung. "Intrusion detection using neural networks and support vector machines." Proceedings of IEEE international joint conference on neural networks. Vol. 2. 2002.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY