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.2026.80485

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

Deep Learning-Based Intrusion Detection System on Edge Network to Detect Industrial Internet of Things Attack

Shrihari Mane[1], Vihas Poojari[2], Kunjan Karawade[3], Aayush Kanigava[4], Prof. Nilesh Patil[5]
[1, 2, 3, 4]*Department of Information Technology, Saraswati College of Engineering, Mumbai, Maharashtra, India*
[5]*Department of Information Technology (Professor), Saraswati College of Engineering, Mumbai, Maharashtra, India*

Abstract: ***This paper presents an AI-based Intrusion Detection System (IDS) for detecting and classifying cyberattacks in network traffic using a balanced dataset with 63 features and 15 attack classes. After preprocessing the data, multiple machine learning and deep learning models were evaluated, where ensemble methods showed better performance for intrusion detection. The final model uses a soft-voting ensemble of XGBoost, Random Forest, and Extra Trees, achieving 93.2% accuracy with a macro precision and weighted F1-score of 0.93. To improve reliability, a confidence threshold mechanism marks uncertain predictions, reducing false alarms in practical deployment. The system is deployed through a Gradio-based interface for real-time analysis, attack prediction, and PDF report generation. This framework offers a practical and efficient AI-driven solution for real-time cybersecurity monitoring.***

Keywords: Intrusion Detection System, Cybersecurity, Ensemble Learning, XGBoost, Network Security, Machine Learning.

I. INTRODUCTION

The rapid growth of digital systems and connected networks has changed the way people communicate, work, and manage important services. From personal communication to banking, healthcare, and industrial operations, modern systems rely heavily on secure network infrastructures. However, this growing dependence on interconnected technologies has also increased exposure to cyber threats. Attacks such as Distributed Denial of Service (DDoS), malware infections, phishing attempts, and unauthorized access have become more frequent and more sophisticated [1], [2]. These attacks can cause major financial losses, disrupt operations, and compromise sensitive information, making network security an essential concern for organizations and individuals.

Traditional security tools such as firewalls and antivirus software are useful for blocking known threats, but they often struggle to detect new or evolving attack patterns. Most of these systems rely on predefined signatures, which limits their ability to identify zero-day attacks or unknown malicious behavior. Because of this limitation, Intrusion Detection Systems (IDS) have become an important part of modern cybersecurity frameworks [3], [4]. An IDS monitors network traffic, identifies suspicious behavior, and helps security teams respond to threats before serious damage occurs. With the advancement of Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning (DL) techniques have shown strong potential in improving intrusion detection capabilities. These methods can learn patterns from network traffic data and identify abnormal activities that may indicate an attack. Unlike rule-based systems, AI-driven IDS models can adapt to changing traffic behavior and detect complex threats with greater efficiency [5], [6]. This makes them highly suitable for modern cybersecurity environments where attack methods constantly evolve. In this work, an AI-based Cyber Intrusion Detection System is developed to classify multiple types of cyber threats in network traffic. The proposed system is designed to detect 15 different attack categories, including DDoS attacks, malware activities, reconnaissance attacks, web-based attacks, and normal traffic behavior. To prepare the data for classification, a preprocessing pipeline is applied that includes handling missing values, feature selection, normalization, and encoding categorical values. These steps ensure that the network traffic data is properly structured for training machine learning models [7].

To identify the most effective detection approach, several machine learning and deep learning models are evaluated, including Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Autoencoder, XGBoost, Random Forest, and Extra Trees. Based on performance comparisons, ensemble learning methods show better results for this structured dataset [8], [9]. Therefore, a soft-voting ensemble model combining XGBoost, Random Forest, and Extra Trees is proposed as the final IDS model. The performance of the model is assessed using evaluation metrics such as accuracy, F1-score, and macro precision to ensure balanced performance across all attack categories.

To improve the reliability of predictions in real-world scenarios, the system also includes a confidence threshold mechanism. Predictions with low confidence are labeled as uncertain, reducing the chance of false alarms and improving trust in the detection results [10]. For practical usability, the IDS is integrated into an interactive interface that allows real-time traffic analysis, attack prediction, and report generation. This makes the system suitable not only for research purposes but also for practical cybersecurity monitoring applications.

The main objective of this research is to develop an effective and practical AI-powered intrusion detection framework that improves the detection of cyber threats while maintaining usability for real-world deployment. By combining data preprocessing, comparative model evaluation, ensemble learning, and real-time deployment, the proposed system contributes toward building a more reliable and intelligent defense mechanism for modern network security.

II. LITERATURE REVIEW

The increasing complexity of cyberattacks has led to significant advancements in Intrusion Detection Systems (IDSs), shifting them from simple rule-based systems to more intelligent and adaptive security solutions. Earlier IDS models mainly depended on signature-based detection methods, where known attack patterns were stored in a database and incoming traffic was matched against those signatures. Although effective for identifying previously known threats, these systems often failed to detect unknown or modified attacks, limiting their usefulness in dynamic threat environments [5]. To overcome this limitation, anomaly-based detection methods were introduced. These systems establish a baseline of normal network behavior and identify deviations from that behavior as possible intrusions, making them more suitable for detecting zero-day attacks and emerging threats [6].

The evolution of cyber threats has significantly influenced the development of Intrusion Detection Systems (IDSs). Early IDS models mainly relied on signature-based detection methods, which were effective for identifying known threats but lacked the ability to detect new or modified attacks [5]. To overcome this limitation, anomaly-based detection methods were introduced, allowing systems to identify suspicious behavior by detecting deviations from normal network activity [6]. This shift laid the foundation for the integration of intelligent techniques in intrusion detection.

A. Machine Learning Approaches in IDS

Machine Learning (ML) has played a major role in improving IDS performance by enabling systems to learn patterns from network traffic data. Traditional models such as Support Vector Machines, Decision Trees, and Naive Bayes have been widely applied for attack classification [7], [8]. Among these methods, ensemble models such as Random Forest and XGBoost have shown better performance because they combine multiple learners to improve prediction accuracy and robustness [9], [10].

B. Deep Learning Approaches in IDS

Deep Learning (DL) approaches have further enhanced intrusion detection by automatically extracting complex features from data. Models like Multi-Layer Perceptron (MLP), Convolutional Neural Networks (CNN), and Autoencoders have been used to identify hidden patterns in network traffic and improve attack detection [11]–[14]. However, these models often require larger datasets and higher computational resources, which can affect their performance in imbalanced cybersecurity datasets.

C. Ensemble Learning for Enhanced IDS Performance

To achieve better detection performance, recent studies have focused on ensemble learning techniques that combine the strengths of multiple models. Methods such as soft voting improve classification reliability by merging probability outputs from different classifiers, resulting in better precision and balanced detection across multiple attack classes [15], [16]. Inspired by these findings, this work applies a soft-voting ensemble approach with a confidence threshold mechanism to improve both detection accuracy and reliability in real-time intrusion detection.

In summary, the literature shows that intrusion detection systems have evolved from basic signature-based methods to intelligent machine learning and deep learning approaches capable of identifying complex cyber threats. Traditional machine learning models provide strong baseline performance, while deep learning models enhance feature extraction capabilities for complex traffic patterns. Recent research indicates that ensemble learning methods offer the most balanced and reliable performance by combining the strengths of multiple classifiers. Based on these observations, the proposed work adopts an ensemble-based IDS framework to achieve accurate, scalable, and dependable intrusion detection for modern cybersecurity environments.

Comparative Summary of Recent Studies on Intrusion Detection Systems for IIoT/Edge Networks

Paper	Dataset(s)	Technology / Model	Research Gap Addressed	Key Findings
Paper 1 (2025)	Edge-IIoTset	EFA + SMOTE + ML models	Traditional ML IDS struggles with tuning and imbalance	EFA outperforms PSO, GA, Firefly
Paper 2 (2024)	Edge-IIoTset	FL + CNN + GRU + LSTM	Centralized IDS affects privacy and scalability	FL improves privacy and detects multiple attacks
Paper 3 (2025)	IIoT datasets	RF, XGBoost, DT, SVC, LR	Lack of model benchmarking	RF best, followed by XGBoost
Paper 4 (2025)	X-IIoTID, WUSTL-IIoT	FL + CNN-BiLSTM	Centralized models lack privacy	Strong results on multiple attacks

III.METHODOLOGY

This section describes the methodology used to design and evaluate the proposed AI-powered Intrusion Detection System (IDS). The framework consists of four stages: data preprocessing, model comparison, ensemble integration, and performance evaluation. These stages were designed to improve detection accuracy while ensuring reliability in real-world cybersecurity applications [9], [10].

A. Data Engineering and Preprocessing

The proposed IDS uses a resampled network traffic dataset containing 63 features and 15 attack classes for multi-class classification. Since raw network traffic data contains redundant and inconsistent values, preprocessing was performed before training [11], [12].

Initially, non-relevant attributes such as timestamps, IP addresses, and payload-related fields were removed to reduce noise and prevent data leakage [13]. Missing or invalid values were then converted into numerical form and replaced with zero to maintain data consistency [14].

Categorical values were encoded using label encoding, and standard normalization was applied so that all features contributed equally during training. The dataset was then divided into 80% training data and 20% testing data using stratified sampling to preserve class balance [15], [16].

B. Comparative Model Development

To identify the best classification approach, both deep learning and machine learning models were tested on the processed dataset [10], [11].

Among the deep learning models, MLP, 1D-CNN, and Autoencoder were evaluated. These models were able to capture non-linear patterns but showed moderate performance due to the structured nature of the dataset [12], [13].

Machine learning models performed better on the tabular data. XGBoost achieved the highest standalone performance, while Random Forest and Extra Trees also showed strong classification capability and robustness [9], [15]. The results indicated that tree-based ensemble models are more suitable than deep learning models for this intrusion detection task [10].

C. *Ensemble Model Integration*

Based on the comparative results, a soft-voting ensemble model was developed using XGBoost, Random Forest, and Extra Trees. In this method, each classifier predicts class probabilities, and the final prediction is determined by averaging these probabilities [15], [16].

This ensemble approach improves prediction stability and reduces the dependency on any single classifier. By combining the strengths of multiple models, the IDS achieves better generalization and balanced detection performance across different attack categories [9], [10].

D. *Performance Evaluation and Reliability Assessment*

The proposed IDS was evaluated using Accuracy, Macro Precision, and Weighted F1-Score, which provide a balanced assessment of multi-class classification performance [11], [14].

To improve reliability, a confidence threshold mechanism was introduced. If the prediction confidence was below 80%, the output was labeled as “Uncertain.” This reduced the chance of false alarms and improved the trustworthiness of the system in practical deployment [16].

By combining ensemble learning with confidence-based validation, the proposed IDS achieves reliable and accurate intrusion detection suitable for real-world cybersecurity monitoring [14], [16].

The methodology follows four main steps: data preprocessing, model evaluation, ensemble learning, and performance validation. The network traffic data is first cleaned and normalized to prepare it for training. Multiple machine learning and deep learning models are then compared, after which the best-performing classifiers are combined using a soft-voting ensemble approach. Finally, the system performance is evaluated using standard metrics, along with a confidence threshold mechanism to improve prediction reliability and reduce false alarms in real-time intrusion detection.

IV. PROPOSED SYSTEM

The proposed Intrusion Detection System (IDS) is designed as a modular framework for processing network traffic, identifying cyber threats, and generating real-time security insights. The architecture consists of five major modules: data input, preprocessing, ensemble detection, prediction validation, and reporting. This modular design improves scalability, detection performance, and usability in practical cybersecurity environments [9], [10].

A. *Input Data Module*

The system accepts network traffic data in CSV format, containing multiple traffic-related features such as packet details, protocol information, and communication attributes. Since raw traffic data may contain redundant and inconsistent information, it is first passed to the preprocessing stage for cleaning and transformation [11].

B. *Preprocessing Module*

The preprocessing module prepares the raw traffic data for classification by applying feature filtering, missing value handling, encoding, and normalization. Irrelevant fields such as timestamps, IP addresses, and payload-related attributes are removed to reduce noise and prevent data leakage [12], [13].

After feature selection, missing values are handled, categorical features are converted into numerical form using label encoding, and standard scaling is applied to normalize all features. These steps improve data quality and ensure that all attributes contribute effectively during classification [14], [15].

C. *Ensemble Detection Module*

The core detection engine combines XGBoost, Random Forest, and Extra Trees classifiers using a soft-voting ensemble mechanism [9], [10].

Each classifier predicts the probability of the input belonging to each attack class. These probability scores are then averaged, and the class with the highest score is selected as the final prediction. This ensemble approach improves detection accuracy, reduces model bias, and enhances classification stability across multiple attack types [15], [16].

D. Prediction Validation Module

To improve reliability, the system evaluates the confidence score of each prediction. If the predicted probability is above 80%, the result is considered reliable; otherwise, it is marked as "Uncertain" [16].

This confidence threshold helps reduce false positives and ensures that uncertain predictions can be reviewed before final action is taken, improving the trustworthiness of the IDS in real-world deployment [14].

E. Reporting and Output Module

The final module presents the detection results through an interactive Gradio-based interface, where users can upload traffic data and receive real-time predictions. The system also generates visual summaries and PDF reports for easier monitoring and analysis [11], [12].

This reporting module improves interpretability by presenting attack predictions, confidence levels, and traffic summaries in a user-friendly format, making the proposed IDS practical for real-time cybersecurity applications.

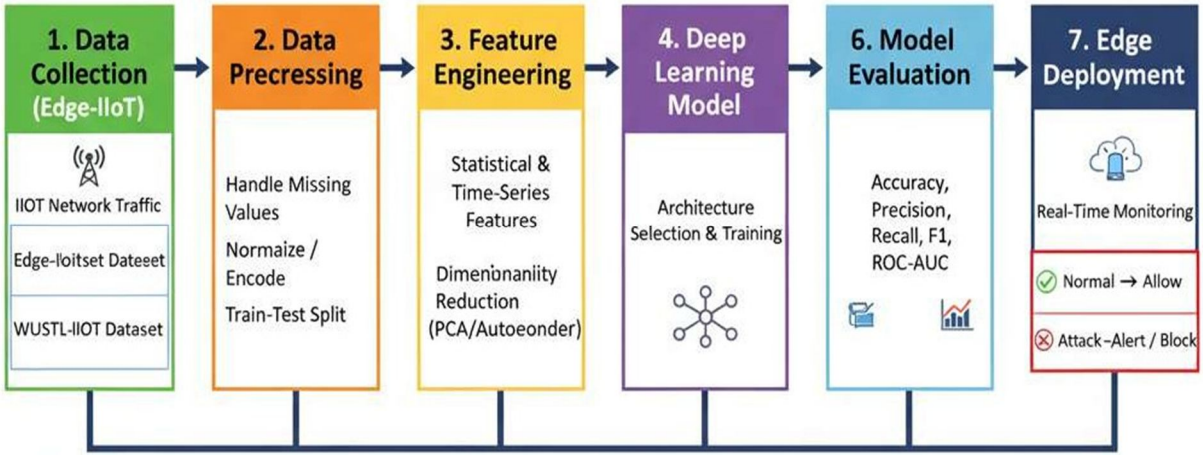


Fig 1. Architecture of the Proposed Ensemble-Based Intrusion Detection System

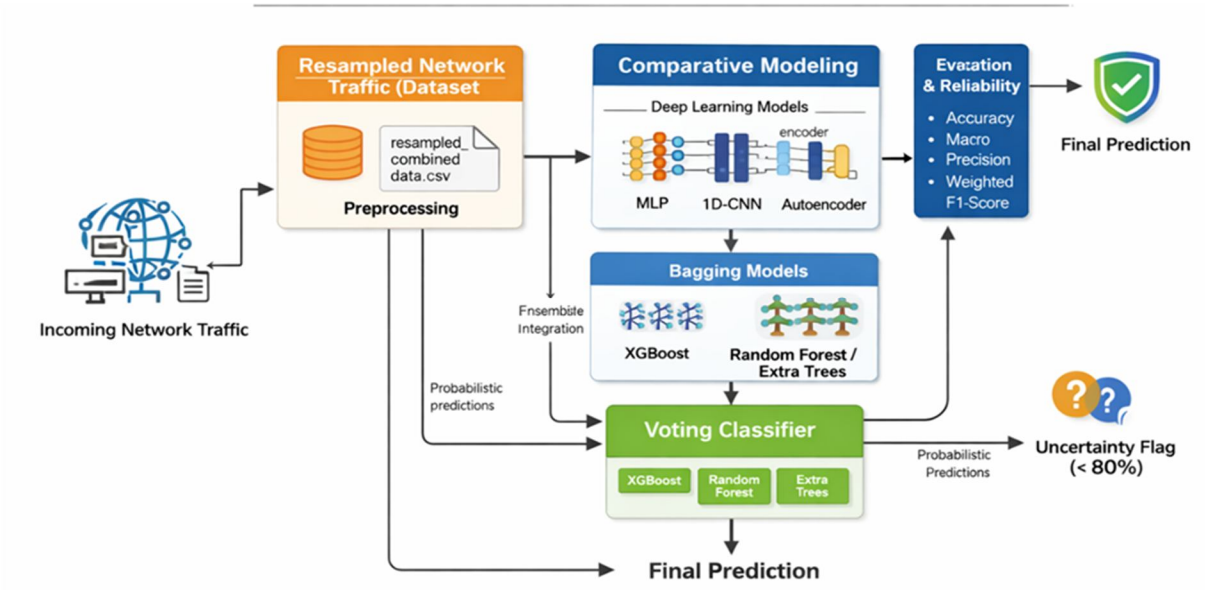


Fig 2. Architecture of the Proposed Ensemble-Based Intrusion Detection System

V. RESULT AND FINDINGS

The developed intrusion detection system was tested using several machine learning and deep learning models to identify the most suitable technique for detecting different cyberattacks in network traffic. The experimental observations showed that ensemble-based machine learning models performed better than deep learning models for the selected dataset.

Among the deep learning models, the MLP model achieved an accuracy of 78%, while the CNN model slightly improved the result with 79% accuracy. The Autoencoder gave the lowest performance, reaching 69% accuracy, which suggests that deep learning models were less effective for this structured tabular data.

The machine learning models provided better outcomes. Random Forest achieved 92% accuracy, while XGBoost reached 93%, making it the strongest individual model. To further improve the performance, these models were combined with Extra Trees in a soft-voting ensemble model, which produced the best results overall.

The final ensemble model achieved 93.2% accuracy, along with a macro precision of 0.93 and a weighted F1-score of 0.93, showing that the system maintained balanced detection performance across multiple attack classes. The confusion matrix also indicated that most traffic samples were classified correctly, with only a few errors between attack categories having similar traffic patterns.

The class-level analysis showed that the system detected attacks such as DDoS, normal traffic, and vulnerability scanning with high effectiveness. However, the detection rate for password attacks and DDoS-HTTP attacks was slightly

lower, mainly because these attacks share similar behavioral characteristics with other traffic classes. Even so, the overall performance remained stable across all attack types.

To improve the reliability of predictions, the system included a confidence threshold mechanism. When the prediction confidence was below 80%, the result was labeled as uncertain instead of assigning a direct attack class. This helped reduce false alarms and made the detection process more dependable for real-time usage.

Overall, the results indicate that the proposed ensemble intrusion detection model offers strong detection accuracy and reliable performance for identifying multiple network attacks. The combination of ensemble learning with confidence-based validation makes the system practical for real-world cybersecurity monitoring.

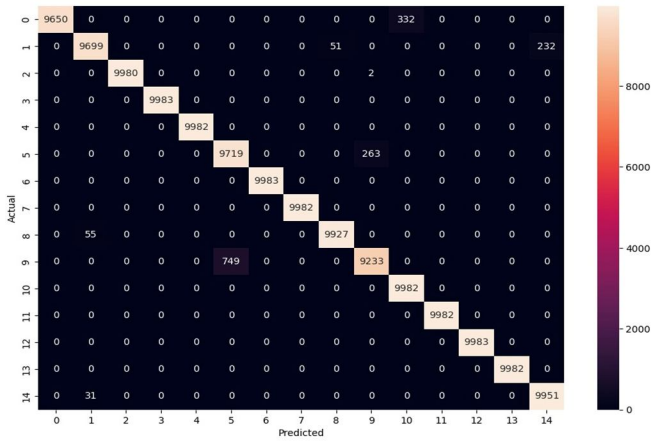


Fig. 3.. Confusion matrix of the proposed ensemble intrusion detection model

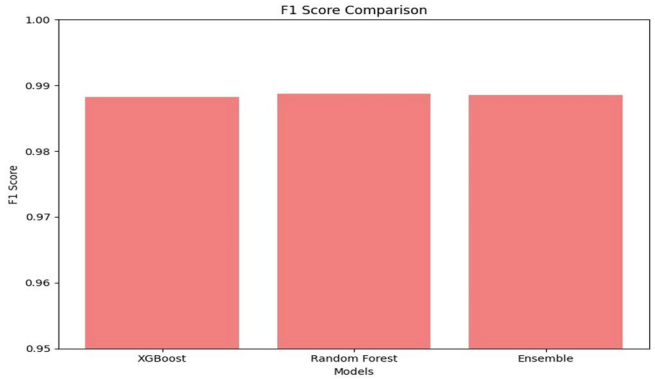


Fig. 4. F1-score comparison of the evaluated classifiers

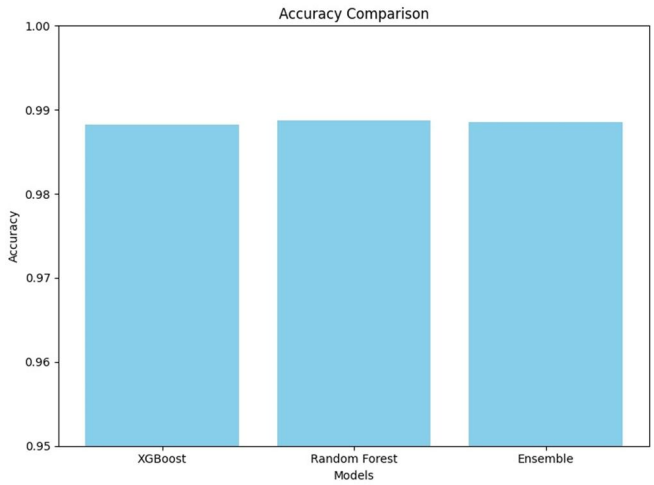


Fig. 5. Accuracy comparison of deep learning and machine learning models

Model	Architecture/Approach	Accuracy
MLP	4-layer Dense (256-128-64)	0.78
CNN	1D-Conv + MaxPool	0.79
Autoencoder	Dimensionality Reduction + Dense	0.69
Random Forest	300 Trees	0.92
XGBoost	Gradient Boosting (Depth 10)	0.93
Ensemble	**Voting (RF + XGB + ExtraTrees)**	**0.93**

Fig. 6. Accuracy comparison of deep learning and machine learning models

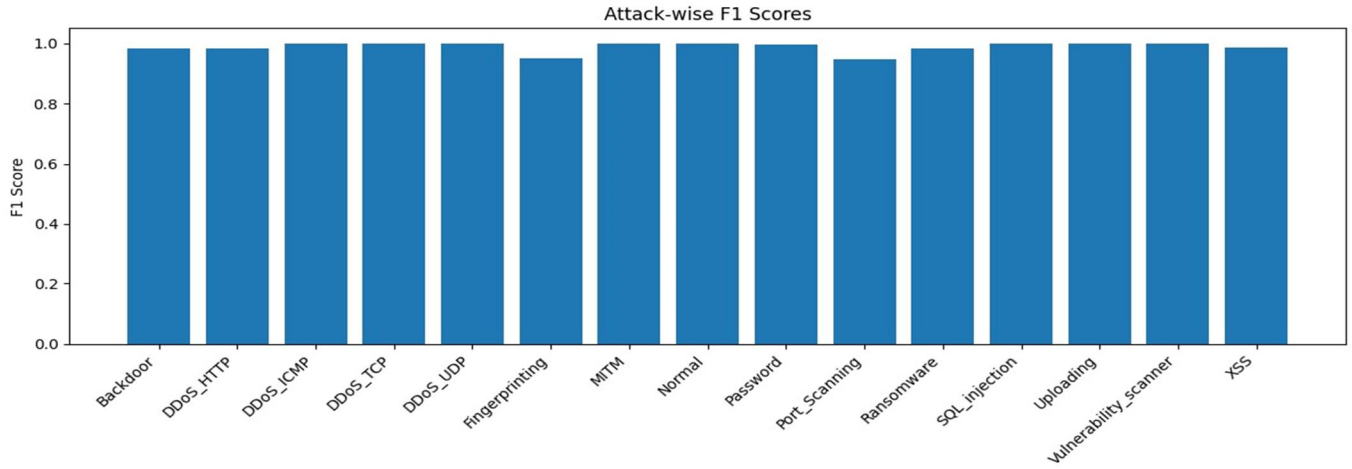


Fig. 7. Attack-wise F1 Scores of the proposed Intrusion Detection Model

VI. CONCLUSION

This research proposed an AI-powered Intrusion Detection System (IDS) for the classification of multiple cyber threats in network traffic using an ensemble learning framework. The system was developed using a structured preprocessing pipeline involving feature selection, missing value handling, label encoding, and normalization to prepare network traffic data for efficient classification. A comparative analysis of deep learning models and ensemble machine learning methods demonstrated that tree-based ensemble models provide superior performance for structured intrusion detection datasets [9], [10].

Based on the comparative evaluation, a soft-voting ensemble model integrating XGBoost, Random Forest, and Extra Trees was implemented as the final detection framework. The proposed model achieved an overall accuracy of 93.2%, along with strong macro precision and weighted F1-score, demonstrating its effectiveness in detecting multiple attack categories while maintaining balanced classification performance [14], [15].

To improve operational reliability, the system incorporated a confidence threshold mechanism that marks low-confidence predictions as uncertain. This enhancement reduces false alarms and improves trustworthiness, making the system more suitable for real-world cybersecurity applications [16].

The experimental results confirm that the proposed ensemble-based IDS provides accurate, reliable, and scalable intrusion detection, making it a practical solution for modern network security environments. By integrating strong predictive performance with real-time usability, this work contributes toward the development of more intelligent and dependable cybersecurity defense systems.

VII. FUTURE SCOPE

Although the proposed intrusion detection system demonstrates strong performance, several improvements can be explored in future work to further enhance its effectiveness and adaptability. One potential direction is the integration of real-time streaming data analysis, allowing the system to process live network traffic rather than relying only on static datasets. This would improve the practical applicability of the IDS in real-world environments where immediate threat detection is essential [11], [12].

Future work may also include the application of advanced deep learning architectures, such as Long Short-Term Memory (LSTM) networks or Transformer-based models, to better capture temporal dependencies in network traffic patterns. These approaches may improve the detection of complex and evolving cyberattacks [13], [14].

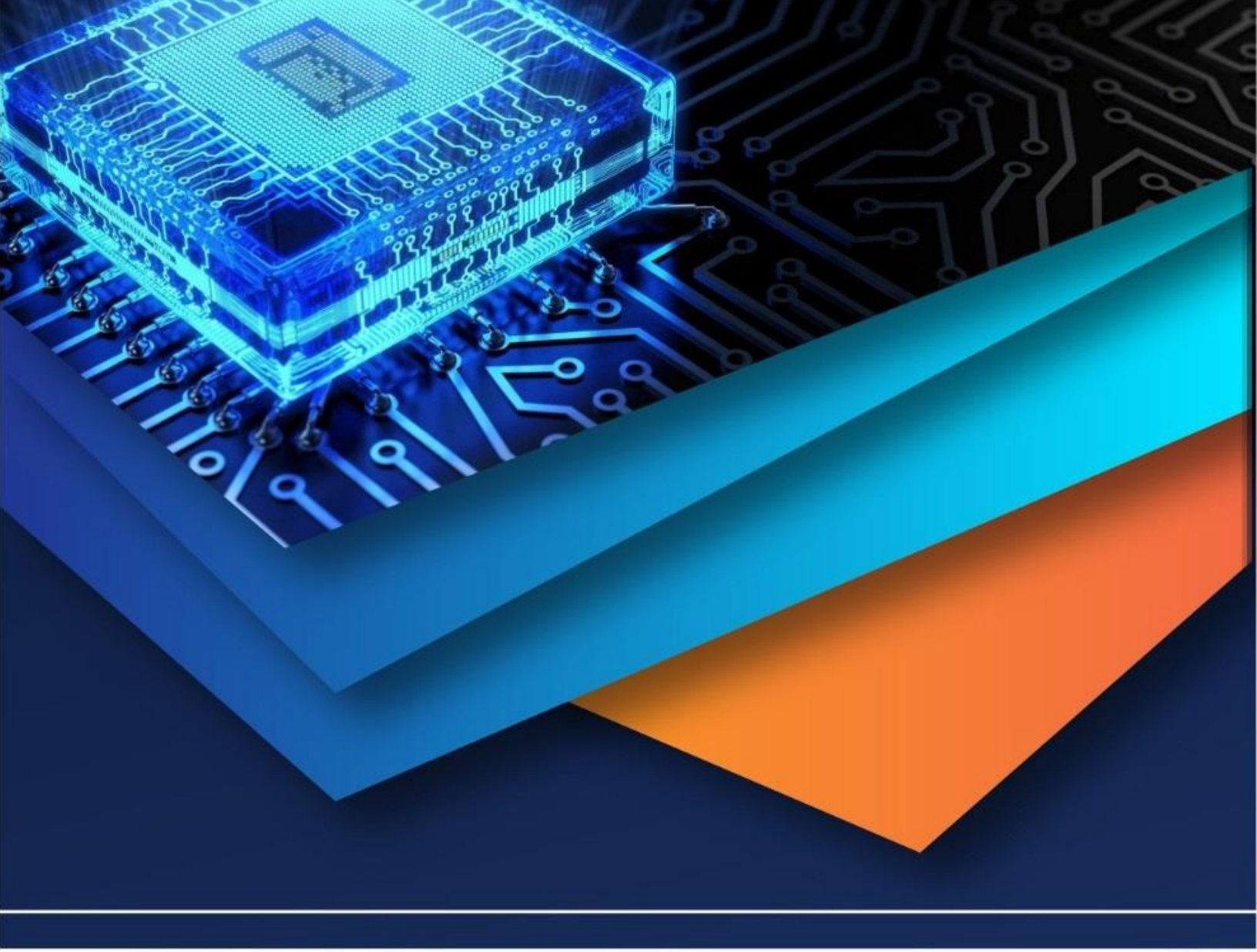
Another enhancement involves the implementation of adaptive learning mechanisms, enabling the IDS to update its detection model dynamically as new attack patterns emerge. This would improve resilience against zero-day threats and reduce performance degradation over time [15].

In addition, integrating the proposed IDS with cloud-based or distributed security frameworks could improve scalability for large-scale enterprise environments. Further improvements in explainability, such as enhanced visualization and interpretable AI techniques, could also help security analysts better understand attack predictions and improve incident response.

These future enhancements can make the proposed IDS more intelligent, adaptive, and effective for next-generation cybersecurity defense systems.

REFERENCES

[1] J. R. Smith and A. L. Johnson, “The evolving landscape of cyber threats,” Journal of Cybersecurity Research, vol. 12, no. 3, pp. 123–145, 2020.
[2] L. Chen and M. Li, “Impact of cyberattacks on critical infrastructure,” in Proceedings of the International Conference on Information Security, 2019, pp. 45–58.
[3] R. Gupta and S. Kumar, “A review of intrusion detection systems,” IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 1–15, 2021.
[4] S. Al-Ghuribi and R. Al-Rubaye, “Machine learning for anomaly detection in cybersecurity: A survey,” Future Generation Computer Systems, vol. 127, pp. 230–245, 2022.
[5] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, 2007.
[6] S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Technical Report, Chalmers University of Technology, 2000.
[7] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in cloud,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.
[8] T. Revathi and A. Malathi, “A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection,” International Journal of Engineering Research & Technology, vol. 2, no. 12, pp. 1848–1853, 2013.
[9] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
[10] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 785–794.
[11] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525–41550, 2019.
[12] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, 2016, pp. 21–26.
[13] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, “Long short term memory recurrent neural network classifier for intrusion detection,” in Proceedings of the International Conference on Platform Technology and Service, 2016, pp. 1–5.
[14] N. 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, 2018.
[15] O. Sagi and L. Rokach, “Ensemble learning: A survey,” Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 8, no. 4, p. e1249, 2018.
[16] R. Polikar, “Ensemble learning,” in Ensemble Machine Learning, Boston, MA, USA: Springer, 2012, pp. 1–34.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY