DeepProbBoost: A Next-Generation Hybrid Deep–Probabilistic Boosting Paradigm for Ultra-Accurate Multi-Level Attack Detection in VANETs

Kalyani Govindam[1], Vemula Arun Kumar[2], Rapaka Vinay[2], T Reddy Koushik Reddy[2], Marka Anuradha[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) play a crucial role in modern Intelligent Transportation Systems by enabling seamless communication among vehicles and infrastructure to enhance road safety and traffic management. With the rapid advancement of wireless technologies such as 5G and the growing adoption of connected and autonomous vehicles, VANET environments have become highly dynamic and data-intensive. Traditional security approaches, including rule-based methods and signature-based Intrusion Detection Systems (IDS), are increasingly inadequate due to their inability to adapt to evolving attack patterns and large-scale data streams. A key challenge lies in accurately identifying malicious nodes in such dynamic networks, where frequent topology changes and strict real-time communication requirements complicate security enforcement. Existing systems often suffer from limitations such as low detection accuracy, high false alarm rates, poor scalability, and ineffective handling of imbalanced datasets. To overcome these challenges, this study proposes a machine learning-driven framework that integrates data preprocessing, exploratory data analysis, and multi-model classification strategies. The framework incorporates models such as Adaptive Boosting Classifier (ABC), Logistic Boosting Classifier (LogitBoost), Gradient Boosting Classifier (GBC), and a novel hybrid ensemble termed Deep Probability Boosting Classifier (DeepProbBoost), which combines Deep Probabilistic Neural Networks (DPNN) with Natural Gradient Boosting (NGB). Furthermore, advanced data balancing techniques, including SMOTE-Tomek and ADASYN, are employed to address class imbalance and improve model generalization. The proposed hybrid boosting approach demonstrates enhanced capability in detecting malicious activities, contributing to scalable, efficient, and reliable security solutions for next-generation vehicular networks.

Key words: Intelligent Transportation Systems, Distributed Denial of Service, Intrusion Detection System, Malicious Node Detection

1. INTRODUCTION

A VANET is a specialized form of Mobile Ad Hoc Network that enables wireless communication among vehicles and between vehicles and roadside infrastructure. Vehicle-to-Vehicle communication supports safety applications such as collision warnings and adaptive driving assistance, but it is highly exposed to malicious nodes that can disrupt communication and compromise road safety [1]. Likewise, Vehicle-to-Infrastructure communication facilitates interaction with traffic control systems and management centers, improving traffic flow and efficiency, yet it remains vulnerable to threats such as spoofing, eavesdropping, and distributed denial of service attacks due to its dependence on open wireless channels [2].

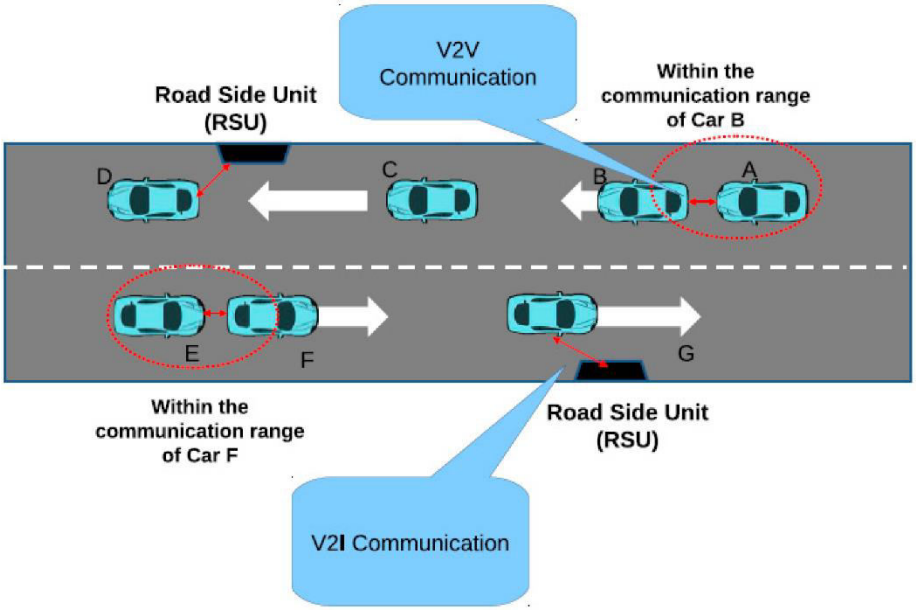

Fig 1. Real time malicious node detection frame work

Fig 1. depicts a malicious traffic detection architecture that integrates monitoring mechanisms with intelligent intrusion detection. As a key component of Intelligent Transportation Systems, VANETs enable real-time information exchange that enhances traffic safety and operational efficiency through applications like emergency alerts and congestion management [3]. However, the decentralized and rapidly changing nature of these networks introduces significant security challenges. Frequent topology changes, high node mobility, and strict latency requirements make it difficult to maintain secure and reliable communication [4]. Among various security threats, distributed denial of service attacks are particularly harmful as they flood the network with excessive traffic, interrupting the delivery of critical safety messages [5]. This can lead to increased packet loss, communication delays, and potential hazards on the road. Conventional security solutions such as firewalls and signature-based IDS are not well-suited for such dynamic environments, as they lack adaptability and real-time responsiveness. Consequently, more advanced, and intelligent approaches are required to address these challenges effectively [6,7]. Recent developments in artificial intelligence and ML have significantly improved the capability to detect and prevent malicious activities in vehicular networks. These techniques allow systems to learn complex patterns from data and distinguish between normal and abnormal behavior with higher accuracy [8]. However, the rapid growth of connected vehicles and the adoption of advanced communication technologies like 5G have expanded the potential attack surface. This has increased the urgency for robust and scalable detection mechanisms to ensure secure communication.

Furthermore, the widespread use of wireless communication in vehicular environments makes it easier for attackers to exploit vulnerabilities and launch coordinated attacks. Although several detection approaches have been proposed, many existing systems still face limitations in scalability, flexibility, and real-time performance [9]. Therefore, there is a critical need for advanced solutions capable of efficiently identifying malicious behavior while maintaining the reliability and efficiency of vehicular communication systems [10]. The increasing complexity of modern network environments has introduced significant challenges in accurately identifying and classifying malicious activities. Traditional security systems often rely on static rules and signatures, which are ineffective against evolving and sophisticated cyberattacks. Additionally, network datasets are typically large, noisy, and imbalanced, making it difficult to distinguish between normal and abnormal behaviour. The presence

of multiple types of attacks further complicates the classification process, as each attack exhibits different characteristics.

2. LITERATURE SURVEY

2.1 Machine Learning-Based Intrusion Detection in Vehicular Networks

Machine learning (ML) techniques have been widely explored for detecting malicious activities in vehicular networks, particularly Distributed Denial of Service (DDoS) attacks. Rashid et al. [11] proposed a real-time malicious node detection system using a distributed multi-layer classifier. Their approach was evaluated using OMNET++ and SUMO simulations, employing ML models such as GBT, LR, MLPC, RF, and SVM to identify attack patterns. Similarly, Kaur et al. [12] simulated DDoS attacks using RaeSE and OMNET++ to analyze network parameters such as packet drop ratio and network access ratio, demonstrating the impact of attacks on communication efficiency. These studies highlight the applicability of ML in identifying network anomalies, though real-time performance remains a challenge.

2.2 CAN Bus Security and Intrusion Detection Systems

In-vehicle network security, particularly Controller Area Network (CAN) bus protection, has gained significant attention. D'Angelo et al. [13] developed a real-time algorithm to classify CAN messages as legitimate or malicious using features such as device fingerprints, clock offsets, and frequency characteristics. Khan et al. [14] proposed an intrusion detection system (IDS) using statistical thresholds and RNN-LSTM classifiers to model ECU fingerprints and detect flooding attacks effectively. Furthermore, Wang et al. [15] combined CNN-based anomaly detection with Kalman filtering to identify abnormal CAN messages without relying on predefined specifications. These approaches demonstrate improved detection accuracy but often require high computational resources and labeled datasets.

2.3 Deep Learning-Based IDS and Performance Limitations

Deep learning models have shown strong potential in handling complex vehicular data. Hyun Min Song et al. [16] proposed a deep convolutional neural network (DCNN)-based IDS for CAN bus protection, capable of processing large-scale data and extracting complex features. Additionally, deep belief networks (DBNs) were explored for unsupervised feature learning, though they suffer from long training times. Zhou et al. [17] highlighted limitations of existing IDS systems, noting that many prioritize detection accuracy while neglecting training and detection time, and fail to effectively integrate CAN IDs with external network data. These limitations hinder their applicability in real-time vehicular environments.

2.4 Authentication and Privacy-Preserving Mechanisms in IoV

Security in the Internet of Vehicles (IoV) also involves authentication and privacy preservation techniques. Omar H.A. et al. [18] proposed an RFID-based authentication mechanism where vehicles communicate with cloud infrastructure for identity verification using electronic tags. Chen Wei et al. [19] introduced a privacy-preserving authentication framework using certificates and pseudonyms issued by trusted authorities. However, these methods face challenges in handling frequent communication delays and scalability in dynamic vehicular environments.

2.5 Blockchain-Based Security in Vehicular Networks

Blockchain technology has emerged as a promising solution for decentralized vehicular security. Wagner M et al. [20] proposed a blockchain-based architecture with locally verified transactions to

secure Vehicular Ad Hoc Networks (VANETs). Their protocol enhances trust and security in environments with limited infrastructure communication. Despite its advantages, blockchain-based approaches may introduce latency and computational overhead, which can impact real-time performance

3. PROPOSED SYSTEM

3.1 Overview

The proposed system as shown in Fig. 2. is a hybrid ML-based framework designed for detecting malicious nodes in VANETs using multiple boosting models. It integrates data preprocessing, EDA, class balancing, and multi-target classification to improve detection accuracy in dynamic environments. The system leverages ensemble learning using ABC, LogitBoost, DeepProbBoost, and GBC to handle complex patterns and imbalanced data effectively, while providing a scalable and real-time prediction interface through a Flask-based deployment.

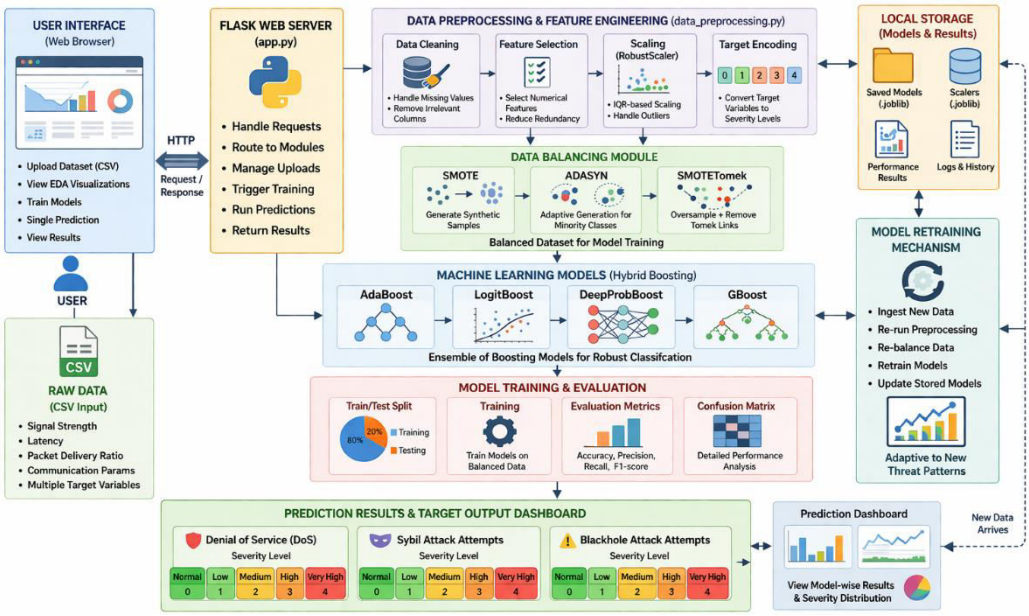

Fig. 2. Proposed system architecture of malicious node detection

User Interface (Web Browser)

- The user interacts with the system through a browser-based graphical interface, designed to simplify complex security monitoring and analysis tasks.
- The interface allows users to upload datasets, visualize EDA outputs, initiate model training, and perform real-time single-instance predictions.
- Dynamic dashboards present analytical visualizations, confusion matrices, and performance metrics for each trained model.
- User actions are translated into HTTP requests and transmitted to the Flask backend for processing and response generation.

Flask Web Server (app.py)

- The Flask server acts as the central control unit, handling all incoming requests and routing them to appropriate processing modules.
- It coordinates dataset ingestion, preprocessing execution, hybrid model training, and prediction workflows.

- The server ensures seamless interaction between frontend components, preprocessing modules, and the ML training engine.
- It also manages file storage, model retrieval, and efficient execution of prediction pipelines in real time.

Local Storage (Models & Results)

- The system maintains structured directories for storing trained models, scalers, and evaluation results.
- Models are serialized using joblib, enabling fast loading without retraining during prediction.
- Scalers specific to each target variable are stored to ensure consistent feature transformation during inference.
- This storage mechanism improves computational efficiency and supports continuous experimentation and comparison.

Raw Data (CSV Input)

- The system accepts structured datasets in CSV format containing vehicular network communication parameters.
- Features include attributes such as signal strength, latency, and other network-level indicators relevant to malicious behavior detection.
- The dataset supports multiple target variables, enabling simultaneous prediction of different attack categories.
- The raw data is directly passed to the preprocessing pipeline for cleaning and transformation.

Data Preprocessing & Feature Engineering (data_preprocessing.py)

- The dataset undergoes preprocessing steps including handling missing values, filtering numerical features, and removing irrelevant attributes.
- RobustScaler is applied to normalize features using interquartile range, effectively handling outliers in dynamic vehicular data.
- Target variables are encoded into categorical severity levels to support multi-class classification tasks.
- The output is a clean and structured dataset optimized for machine learning model training.

Data Balancing Module

- The system incorporates advanced imbalance handling techniques such as SMOTE, ADASYN, and SMOTE Tomek.
- These techniques generate synthetic samples for minority attack classes to balance the dataset distribution.
- SMOTE Tomek further refines class boundaries by removing overlapping noisy samples, improving classification clarity.
- This module significantly enhances detection capability for rare but critical attack events.

ML Models (ABC, LogitBoost, DeepProbBoost, GBC)

- The processed dataset is fed into a set of boosting-based ensemble models for robust classification.
- ABC focuses on sequential error correction, while LogitBoost enhances performance using logistic regression as the base learner.
- GBC captures complex non-linear relationships through gradient-based optimization.

- DeepProbBoost introduces deep probabilistic learning to improve predictive robustness in highly dynamic environments.

Model Training & Evaluation

- The dataset is split into training and testing sets to ensure reliable performance validation.
- Each model is trained on balanced data and evaluated using unseen test samples.
- Performance metrics such as Accuracy, Precision, Recall, and F1-score are computed for each target variable.
- Confusion matrices and classification reports provide detailed insights into model effectiveness across attack classes.

Prediction Results & Target Output

- The trained system performs multi-target prediction for key attack categories: Denial of Service (DoS), Sybil Attack Attempts, Blackhole Attack Attempts
- Predictions are generated using all trained models and displayed in a structured format in the UI.
- The output helps identify malicious nodes and assess the severity level of attacks.
- This enables proactive decision-making for secure vehicular communication systems.

Model Retraining Mechanism

- The system supports iterative retraining using newly uploaded datasets to adapt to evolving network behaviors.
- Updated data is processed through the same preprocessing and balancing pipeline to maintain consistency.
- Existing models can be reloaded or replaced with newly trained versions for improved performance.
- This adaptive capability ensures long-term robustness against emerging and zero-day attack patterns

3.2 DeepProbBoost model

DeepProbBoost is an advanced hybrid boosting model that integrates probabilistic boosting principles with deep learning-based representation capabilities to enhance classification performance in complex and dynamic environments such as VANETs. Unlike traditional boosting methods that rely solely on shallow learners, DeepProbBoost leverages deep feature transformations along with iterative boosting to model highly non-linear relationships in the data. It operates by sequentially refining probabilistic predictions, where each iteration focuses on minimizing uncertainty and correcting previous prediction errors. This probabilistic boosting framework enables the model to handle noisy, imbalanced, and high-dimensional data more effectively, making it highly suitable for multi-target malicious node detection tasks, as illustrated in Fig. 3.

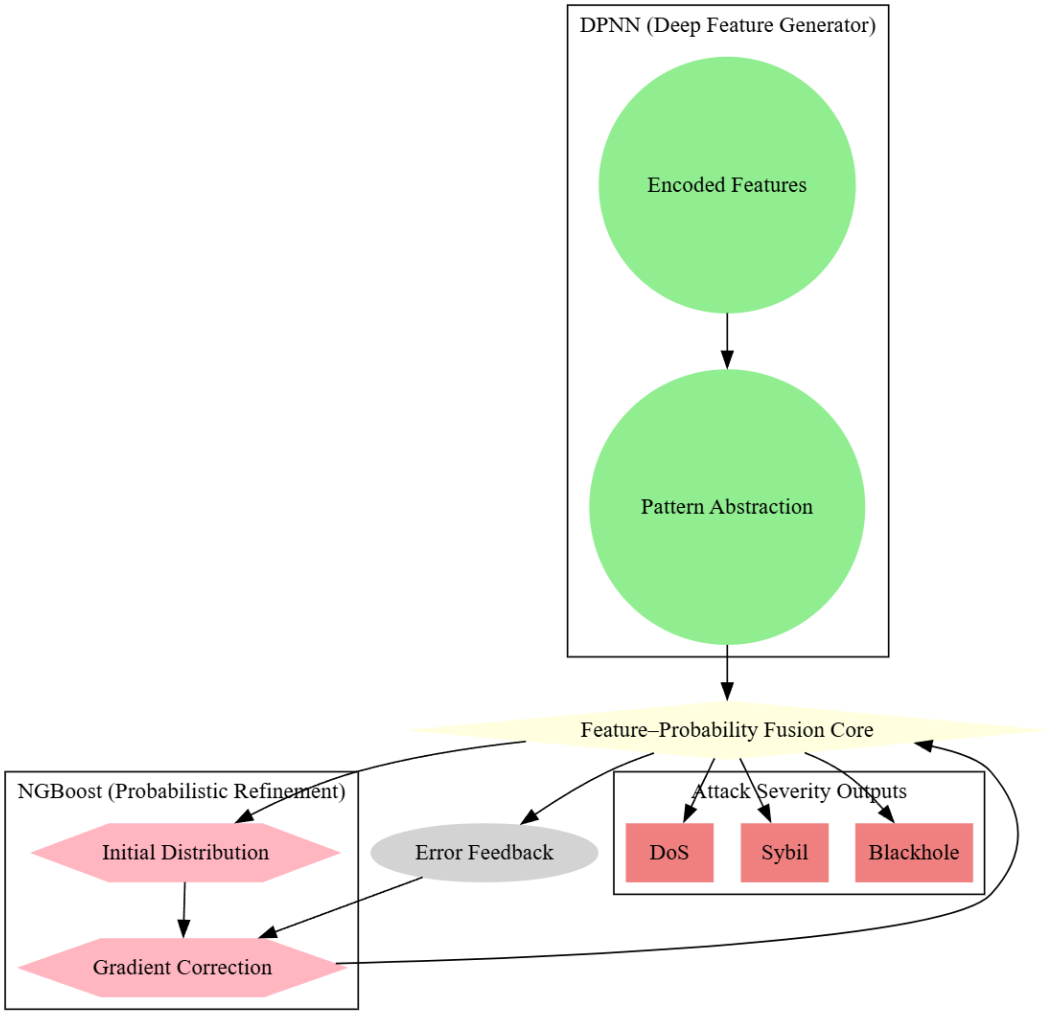

Fig 3. Internal workflow of DeepProbBoost model

The model begins by initializing probability distributions over the target classes. These initial probabilities represent a baseline understanding of class likelihoods before learning begins. Input data is passed through a deep transformation stage, where complex feature representations are extracted. This step enhances the model's ability to capture hidden patterns and dependencies in vehicular network data. The model calculates residual errors in terms of probability differences between actual labels and predicted outputs. These residuals guide subsequent learners in reducing uncertainty. A boosting learner is trained on the transformed features and probabilistic residuals. This learner focuses on correcting the mistakes made by previous iterations while maintaining probabilistic consistency.

The predictions from each learner are integrated into the overall model by updating probability distributions. This ensures that each iteration refines the confidence of predictions rather than just class labels. The process of feature transformation, residual computation, and boosting is repeated iteratively. Each cycle improves both feature representation and classification accuracy. The final output is generated as a probability distribution over classes. The class with the highest probability is selected as the prediction, while probability scores provide additional interpretability.

4. RESULT DESCRIPTION

The results section presents the performance evaluation of the developed system in detecting malicious nodes within vehicular network data. It highlights how different ML models perform when applied to

the processed and balanced dataset. The evaluation is carried out using key metrics such as accuracy, precision, recall, and F1-score to ensure a comprehensive analysis. Comparative results are used to identify the most effective model among KNN, SVC, GNB, and STT. The outcomes demonstrate the impact of preprocessing and data balancing techniques on improving prediction reliability. Visualizations and performance metrics further support the analysis of model behaviour.

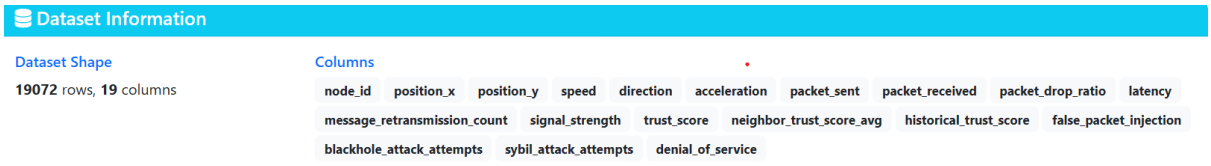

Fig. 4. Dataset information overview

Fig. 4. depicts the EDA interface presenting detailed dataset information used for malicious node detection. The figure highlights the overall structure of the dataset, including the total number of records and features available for analysis. It showcases various attributes such as node identifiers, positional coordinates, communication metrics, and trust-related parameters that are essential for understanding network behaviour. The inclusion of features like latency, signal strength, packet transmission, and trust scores indicates the comprehensive nature of the dataset. Additionally, the presence of target variables such as denial_of_service, sybil_attack_attempts, and blackhole_attack_attempts reflects the system's capability to analyse multiple attack types.

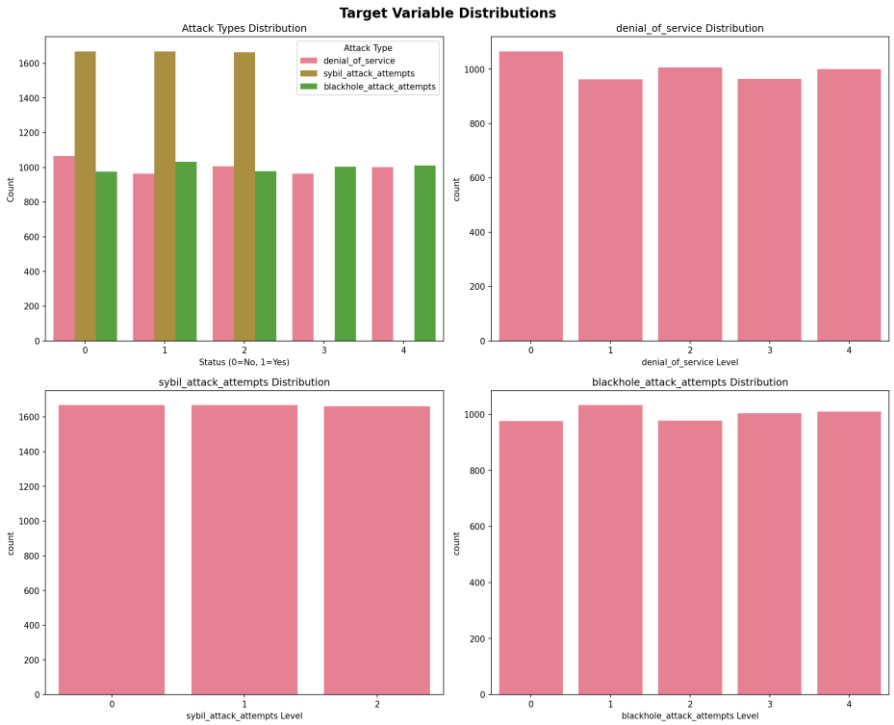

Fig. 5. Target variable distributions

Fig. 5. illustrates the distribution of target variables used for detecting malicious activities in the vehicular network dataset. The figure presents multiple plots showing the frequency of different attack categories, including denial_of_service, sybil_attack_attempts, and blackhole_attack_attempts. It depicts how the data is distributed across various severity levels, providing insight into class balance and variation among attack types. The visualization highlights the presence of multiple classes for each

target, indicating the complexity of the classification problem. It also helps in identifying whether the dataset is balanced or skewed across different attack levels.

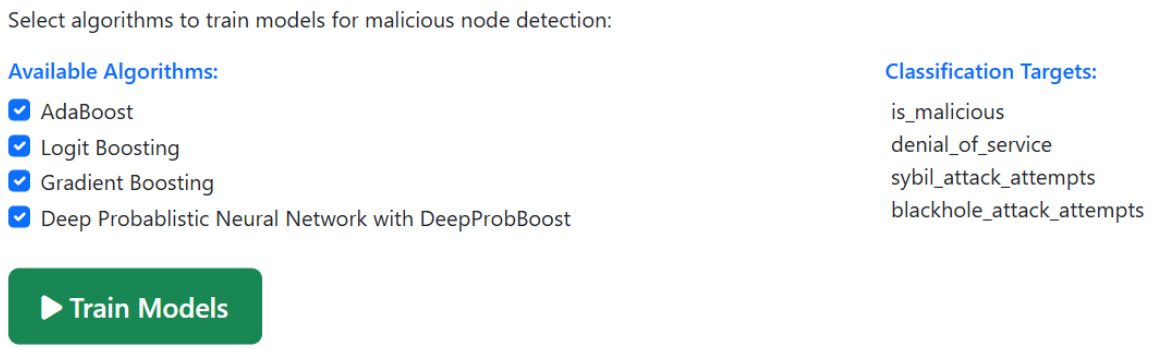

Fig. 6. ML model training interface

Fig. 6. illustrates the model training interface of the malicious node detection system, where multiple ML algorithms can be selected for classification tasks. The figure depicts the availability of models such as ABC, GBC, LogitBoost, and DeepProbBoost, enabling a comparative learning approach for improved prediction accuracy. It also highlights the classification targets including is_malicious, denial_of_service, sybil_attack_attempts, and blackhole_attack_attempts, indicating the multi-target nature of the system. The interface allows users to initiate the training process by selecting appropriate algorithms based on requirements. This setup supports flexible experimentation and evaluation of different models on the same dataset.

Fig 7. shows confusion matrix for the DeepProbBoost model on the denial_of_service target demonstrates highly accurate and well-balanced classification across all severity levels. The strong concentration of values along the diagonal indicates that the model correctly predicts Normal, Medium, High, and Very High classes with minimal misclassification. Unlike other models, errors are very low and only occur slightly between neighboring classes, showing excellent class separation and robustness. This highlights the effectiveness of the DeepProbBoost architecture, where deep feature extraction and probabilistic refinement enable precise detection of attack intensity, making it the most reliable model among all evaluated approaches.

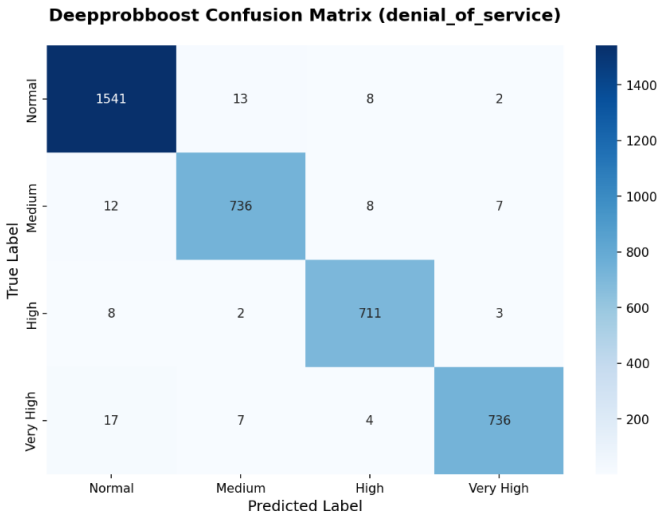

Fig 7. Illustration of confusion matrix using proposed DeepProbBoost model for Dos attack

Fig 8. illustrates confusion matrix for the DeepProbBoost on the sybil_attack_attempts target shows excellent classification performance with very high accuracy across all classes. The dominant diagonal values indicate that the model correctly predicts Normal, Low, and Medium categories with minimal misclassification. Only a few instances are incorrectly classified into neighboring classes, demonstrating strong class separation and precise learning of attack patterns. This highlights the effectiveness of DeepProbBoost in capturing subtle differences in Sybil attack intensity, making it the most reliable and robust model compared to the others.

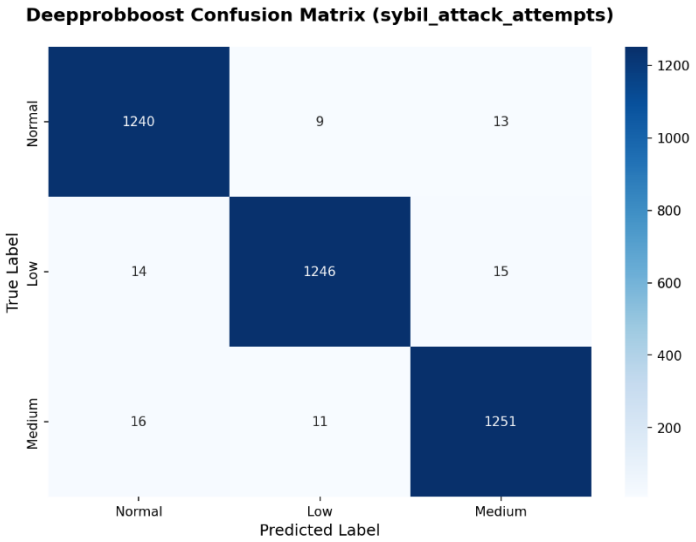

Fig 8. Illustration of confusion matrix using proposed DeepProbBoost model

Fig 9. illustrates the confusion matrix for the DeepProbBoost on the blackhole_attack_attempts target demonstrates excellent classification performance with very high accuracy across all severity levels. The strong diagonal dominance indicates that the model correctly identifies Normal, Low, Medium, High, and Very High classes with minimal errors. Misclassifications are very few and mostly limited to adjacent classes, showing clear separation between different attack intensities. This confirms that DeepProbBoost effectively captures complex blackhole attack patterns and provides highly reliable and precise predictions compared to other models.

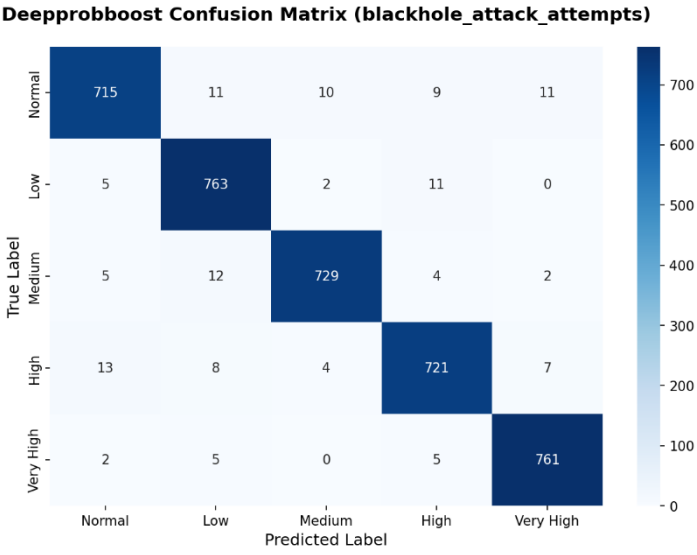

Fig 9. Illustration of confusion matrix using proposed DeepProbBoost model

The comparison table 1 for Denial of Service (DoS) clearly highlights the superior performance of the proposed DeepProbBoost model over all other baseline approaches. ABC shows very poor performance, with low accuracy (20.47%) and an extremely low F1-score (7.90%), indicating its inability to correctly capture varying DoS severity levels. LogitBoost demonstrates slight improvement with better precision (32.40%), but still suffers from inconsistent recall and overall weak classification capability. GBC significantly outperforms both ABC and LogitBoost, achieving moderate accuracy (50.25%) and balanced precision–recall values, showing its ability to better model non-linear patterns in the data. However, the proposed DeepProbBoost model dramatically surpasses all others, achieving near-perfect performance with 97.61% accuracy, precision, recall, and F1-score. This exceptional result confirms that the integration of deep feature extraction and probabilistic boosting enables highly accurate and robust detection of DoS attack intensities, making DeepProbBoost the most effective model for this task.

Table. 1: Comparison table of all the models for Denial of Service (DoS)

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
ABC	20.47%	15.06%	20.47%	7.90%
LogitBoost	25.85%	32.40%	25.85%	25.64%
GBC	50.25%	55.00%	50.25%	50.57%
DeepProbBoost	97.61%	97.62%	97.61%	97.61%

The comparison table 2 shows that for **Sybil attack attempts** clearly demonstrates the varying effectiveness of different models, with the proposed DeepProbBoost model significantly outperforming the others. ABC shows limited performance, with low accuracy (34.65%) and a particularly poor F1-score (21.13%), indicating weak capability in distinguishing different Sybil attack intensity levels. LogitBoost provides slightly more balanced results, with nearly equal precision, recall, and F1-score (~33%), but overall performance remains low, reflecting difficulty in achieving reliable classification. GBC exhibits a noticeable improvement, achieving moderate accuracy (56.49%) along with balanced precision and recall, indicating better learning of Sybil attack patterns. However, the proposed DeepProbBoost model clearly dominates, achieving an outstanding 97.96% across all metrics. This near-perfect performance highlights its ability to effectively capture complex behavioral patterns and accurately classify different levels of Sybil attacks, making it the most robust and reliable model among all evaluated approaches.

Table. 2: Comparison table of all the models for Sybil attack attempts

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
ABC	34.65%	40.13%	34.65%	21.13%
LogitBoost	33.24%	33.25%	33.24%	33.23%
GBC	56.49%	56.55%	56.49%	56.43%
DeepProbBoost	97.96%	97.96%	97.96%	97.96%

Table. 3: Comparison table of all the models for Blackhole Attack Attempts

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
ABC	20.00%	21.64%	20.00%	7.06%
LogitBoost	21.02%	21.00%	21.02%	21.00%
GBC	50.93%	51.07%	50.93%	50.92%
DeepProbBoost	96.70%	96.70%	96.70%	96.69%

The comparison table 3 depicts that for Blackhole Attack Attempts a significant performance gap is shown between traditional boosting models and the proposed DeepProbBoost model. ABC performs poorly, with very low accuracy (20.00%) and an extremely weak F1-score (7.06%), indicating its inability to correctly identify and differentiate blackhole attack severity levels. LogitBoost shows only marginal improvement, with slightly better but still low and inconsistent performance across all metrics (~21%), reflecting weak classification capability. GBC demonstrates a notable improvement, achieving moderate accuracy (50.93%) and balanced precision, recall, and F1-score, indicating its ability to better capture underlying attack patterns compared to the other baseline models. However, the proposed DeepProbBoost model significantly outperforms all others, achieving an impressive 96.70% across accuracy, precision, recall, and F1-score. This highlights its strong capability in modeling complex blackhole attack behaviors and accurately distinguishing between different severity levels, making it the most reliable and effective model for this task.

5. CONCLUSION

The research successfully presents an intelligent and robust framework for detecting malicious behavior in high-mobility vehicular networks by leveraging advanced boosting-based models and a hybrid architecture. The system integrates efficient preprocessing, feature scaling, and data balancing techniques to handle complex and imbalanced network data, followed by the application of multiple models such as ABC, LogitBoost, GBC, and the proposed DeepProbBoost. Experimental results across DoS, Sybil, and Blackhole attack scenarios clearly demonstrate that while traditional models struggle with accurate severity-level classification, the proposed DeepProbBoost consistently achieves superior performance with near-perfect accuracy and balanced precision, recall, and F1-scores. Its ability to effectively capture deep feature representations and refine them through probabilistic learning enables precise detection of attack intensities with minimal misclassification. The deployment of the system through a Flask-based interface further ensures real-time usability, scalability, and ease of interaction. The framework provides a highly reliable, adaptive, and efficient solution for securing vehicular communication environments, making it a strong candidate for real-world intelligent transportation system applications.

REFERENCES

[1] Rashid, K.; Saeed, Y.; Ali, A.; Jamil, F.; Alkanhel, R.; Muthanna, A. An Adaptive Real-Time Malicious Node Detection Framework Using ML in Vehicular Ad-Hoc Networks (VANETs). Sensors 2023, 23, 2594. https://doi.org/10.3390/s23052594

[2] Al-Omaisi, H.; Sundararajan, E.A.; Abdullah, N.F. Towards vanet-ndn: A framework for an efficient data dissemination design scheme. In Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 9–10 July 2019; pp. 412–417.

[3] Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. Comput. Networds 2018, 134, 78–92.

[4] Lee, M.; Atkison, T. Vanet applications: Past, present, and future. Veh. Commun. 2021, 28, 100310.

[5] Sharma, A.; Pandey, K. Recent Advancements in Techniques Used to Solve the RSU Deployment Problem in VANETs: A Comprehensive Survey. Int. J. Sens. Wirel. Commun. Control 2022, 12, 184–193.

[6] Ganesh, A.; Ayyasamy, S. Enhanced Approach in VANETs for Avoidance of Collision with Reinforcement Learning Strategy. In Proceedings of the International Conference on Artificial Intelligence for Smart Community, Perak, Malaysia, 17–18 December 2020; Springer: Berlin/Heidelberg, Germany, 2022; pp. 419–428.

[7] Pandey, P.K.; Kansal, V.; Swaroop, A. VANETs: Architecture, challenges, and applications. In Handling Priority Inversion in Time-Constrained Distributed Databases; IGI Global: Hershey, PA, USA, 2020; pp. 224–239.

[8] Ali, I.; Hassan, A.; Li, F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. Veh. Commun. 2019, 16, 45–61.

[9] Mansoor, S.; Shahid, S.; Ashiq, K.; Alwadai, N.; Javed, M.; Iqbal, S.; Ibrahium, H.A. Controlled growth of nanocomposite thin layer based on Zn-Doped MgO nanoparticles through Sol-Gel technique for biosensor applications. Inorg. Chem. Commun. 2022, 142, 109702.

[10] Gaurav, A.; Gupta, B.B.; Peñalvo, F.J.G.; Nedjah, N.; Psannis, K. Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks. In Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions; Springer: Berlin/Heidelberg, Germany, 2022; pp. 263–278.

[11] Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Veh. Commun. 2022, 34, 100458.

[12] Raza, A.; Bukhari, S.H.R.; Aadil, F.; Iqbal, Z. An UAV-assisted VANET architecture for intelligent transportation system in smart cities. Int. J. Distrib. Sens. Netw. 2021, 17, 15501477211031750.

[13] D'Angelo, G.; Castiglione, A.; Palmieri, F. A Cluster-Based Multidimensional Approach for Detecting Attacks on Connected Vehicles. IEEE Internet Things J. 2021, 8, 12518–12527.

[14] Khan, J.; Lim, D.-W.; Kim, Y.-S. Intrusion Detection System CAN-Bus In-Vehicle Networks Based on the Statistical Characteristics of Attacks. Sensors 2023, 23, 3554.

[15] Wang Liu, S.; Liu, L.; Tang, J.; Yu, B.; Wang, Y.; Shi, W. Edge Computing for Autonomous Driving: Opportunities and Challenges. Proc. IEEE 2019, 107, 1697–1716.

[16] Song, H.M.; Woo, J.; Kim, H.K. In-vehicle network intrusion detection using deep convolutional neural network. Veh. Commun. 2020, 21, 100198.

[17] Abboud, K.; Omar, H.A.; Zhuang, W. Inter working of DSRC and Cellular Network Technologies for V2X Communications: A Survey. IEEE Trans. Veh. Technol. 2016, 65, 9457–9470.

[18] Zhongmei, L.; Wei, C.; Jie, W.; Haitao, Y. Very low latency and high reliability communication of Internet of Vehicles: Status and Outlook. Signal Process. 2019, 35, 1773–1783.

[19] Arushi, A.; Kumar, Y.S. Block Chain Based Security Mechanism for Internet of Vehicles (IoV). In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), Jaipur, India, 26–27 March 2018; pp. 267–272.

[20] Wagner, M.; Mcmillin, B. Cyber-Physical Transactions: A Method for Securing VANETs with Blockchains. In Proceedings of the IEEE Pacific Rim International, Symposium on Dependable Computing, Taipei, Taiwan, 4–7 December 2018; pp. 64–73.