

GUARDEV: Guided Unified Adaptive Response for Defending Electric Vehicles

Koustav Kumar Mondal[1(✉)] and Debasis Das[2]

[1] Inter-Disciplinary Research Division - IoT and Applications, Indian Institute of Technology Jodhpur, Jodhpur, Rajasthan, India
mondal.4@iitj.ac.in

[2] Department of Computer Science Engineering, Indian Institute of Technology Jodhpur, Jodhpur, Rajasthan, India
debasis@iitj.ac.in

Abstract. In the rapidly evolving landscape of electric vehicles (EVs), integrating the Internet of Vehicles (IoV) has opened up new dimensions in automotive technology. While enhancing vehicle performance, safety, and security, this advancement also exposes EVs to heightened cyber threats. To address this critical concern, we introduce GUARDEV: Guided Unified Adaptive Response for Defending Electric Vehicles, a novel Machine Learning (ML)-enhanced conflict resolution-based ensemble Intrusion Detection System (IDS) architecture. GUARDEV leverages the power of adaptive ML techniques to provide a unified and guided response in safeguarding EVs against sophisticated cyber-attacks. Our framework evaluates the effectiveness of three prominent ML models - XGBoost, Random Forest, and Extra Trees - in detecting specific categories of cyber threats. By harnessing the prediction confidence scores from these models, GUARDEV offers a nuanced and intelligent approach to recognizing and thwarting diverse cyber-attacks. Our research, grounded in rigorous experimentation using public IoV security datasets, demonstrates GUARDEV's exceptional accuracy of 99.47% in intrusion detection. This remarkable achievement not only underscores the potential of ML in enhancing vehicular cybersecurity but also establishes GUARDEV as a powerful tool for creating safer, more secure EVs. GUARDEV paves the way for robust protection of internet-connected electric vehicles in today's digital age by providing a guided, unified, and adaptive response to cyber threats.

Keywords: Intrusion Detection System · Electric Vehicle · Internet of Vehicle · Conflict Resolution · Ensemble Learning

1 Introduction

The fusion of the Internet of Things (IoT) with Electric Vehicles (EVs) has led to the emergence of the Internet of Vehicles (IoV) [22], revolutionizing the transportation sector and paving the way for a smarter, more integrated future on

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
A. Antonacopoulos et al. (Eds.): ICPR 2024, LNCS 15324, pp. 47–62, 2025.
https://doi.org/10.1007/978-3-031-78383-8_4

wheels [5]. At the core of this transformation lies the Controller Area Network (CAN) bus within EVs, serving as a vital communication hub linking Electronic Control Units (ECUs) to coordinate various vehicular functions. Additionally, the burgeoning Vehicle-To-Everything (V2X) technology expands this communication network beyond the vehicle, connecting EVs with a diverse array of IoT devices, from roadside infrastructure to smart gadgets [22].

1.1 Motivation

In the rapidly evolving landscape of automotive technology, the convergence of IoT with EVs heralds a new era of connectivity, promising numerous advancements in functionality and convenience. However, this wave of innovation brings with it a critical challenge: the need for robust cybersecurity measures. The integration of IoT into EVs amplifies connectivity but also exposes vulnerabilities within the Internal Vehicular Network (IVN), particularly due to the inherent simplicity of CAN packets lacking encryption or authentication. The potential threats are diverse and significant, ranging from DDoS and Brute Force attacks to Spoofing, DoS, Recon, Web-based intrusions, and the notorious Mirai botnet. As EVs increasingly interface with external networks, the scope of vulnerability expands, necessitating an intelligent, adaptive, and unified approach to fortify cyber defenses and mitigate risks.

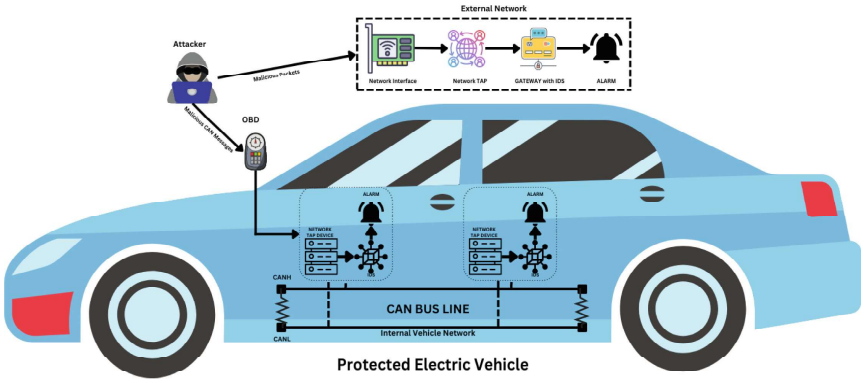


Fig. 1. State of The Art Intrusion Detection System for Electric Vehicle

To address these challenges, we introduce GUARDEV: Guided Unified Adaptive Response for Defending Electric Vehicles. As illustrated in Fig. 1, GUARDEV represents a significant advancement in automotive cybersecurity, offering a comprehensive framework for protecting EVs against cyber threats. This innovative system embodies a proactive approach, leveraging machine learning techniques to provide real-time monitoring, adaptive threat detection, and guided response capabilities. GUARDEV's unified architecture integrates various components of vehicle security, ensuring a cohesive defense strategy. Its adaptive nature allows it to evolve with emerging threats, continuously learning and improving its detection and response mechanisms. The guided aspect

of GUARDEV ensures that responses to detected threats are optimized and contextually appropriate, minimizing false positives and enhancing overall system efficiency. By implementing GUARDEV, we aim to create a robust, intelligent defense system that not only protects against known cyber threats but also adapts to new, unforeseen challenges in the ever-evolving landscape of EV cybersecurity. This approach is crucial in ensuring the resilience and safety of IoT-integrated EVs, paving the way for a secure and connected automotive future.

1.2 Problem Statement

In the context of rapidly evolving cyber threats to Electric Vehicles (EVs), recent advancements in Machine Learning (ML) have sparked considerable interest in enhancing cybersecurity measures, particularly through Intrusion Detection Systems (IDSs). While ML techniques offer promising avenues for bolstering automotive cybersecurity by analyzing network traffic data, their effectiveness varies significantly across different types of cyber-attacks. This variability poses a critical challenge to ensuring the reliability and robustness of IDSs in real-world automotive environments. Moreover, issues such as data scarcity, model interpretability, and vulnerability to adversarial attacks complicate the deployment of ML-driven IDSs in automotive systems. Addressing these complexities is crucial for enhancing the resilience and effectiveness of cybersecurity measures in connected EVs, ultimately ensuring the safety and security of future automotive ecosystems. To tackle these challenges, we introduce GUARDEV: Guided Unified Adaptive Response for Defending Electric Vehicles. This novel framework harnesses the power of advanced ML algorithms, including Extreme Gradient Boosting (XGBoost) [17], Random Forest Classifier [9], and Extra Trees Classifier [18]. GUARDEV aims to achieve optimal performance with reduced execution time across various cyber-attack types by providing a guided, unified, and adaptive response to threats.

1.3 Contributions

This study contributes significantly to the field of EV cybersecurity in three key ways:

1. **Development of GUARDEV Architecture:** We introduce GUARDEV, a guided unified adaptive response framework for defending electric vehicles. This architecture employs a unique combination of balanced weight class and confidence decision techniques, specifically designed for efficient intrusion detection in EVs. By integrating multiple ML models into a unified framework, GUARDEV enhances the robustness and reliability of intrusion detection systems in automotive environments while providing guided and adaptive responses to threats.
2. **Rigorous Testing on Cutting-Edge IoT Datasets:** GUARDEV undergoes rigorous testing on the CICIoT2023 [16] Dataset, which represents a wide spectrum of both internal and external network scenarios. By evaluating the

performance of our framework on this dataset, we ensure its applicability and effectiveness across real-world cyber-attack scenarios encountered in automotive systems, demonstrating the adaptive nature of GUARDEV.
3. **Benchmarking Against State-of-the-Art Methodologies:** We benchmark GUARDEV's performance against other state-of-the-art methodologies, showcasing its superiority in EV cybersecurity. Through comparative analysis and comprehensive evaluation, we demonstrate the effectiveness and efficacy of our guided and unified approach in mitigating cyber threats and enhancing the security posture of electric vehicles.

2 Brief Literature Review

This section explores the current landscape of cybersecurity for Electric Vehicles (EVs) and the Internet of Vehicles (IoV), reviewing recent advancements and identifying gaps in Intrusion Detection Systems (IDSs). While various innovative approaches using machine learning and deep learning techniques have emerged, the challenge of developing a guided, unified, and adaptive response system for IoV-enabled EVs remains.

2.1 Deep Learning Approaches in IDS

Song et al. [20] and Agrawal et al. [1] focused on deep learning-based IDSs, with Song et al. developing a convolutional neural network model for car-hacking detection and Agrawal et al. proposing a novel system for various attack types. While effective, these approaches lack the unified and adaptive response mechanism that GUARDEV aims to provide. Awajan [7] presented a Deep Learning-based IDS for IoT devices, achieving high precision, recall, and F1-scores, but did not specifically address the guided response needs of IoV scenarios.

2.2 Ensemble and Hybrid Models

Elmasry et al. [13] and Chen et al. [11] introduced ensemble models for network intrusion detection, using combinations of various neural network architectures. While innovative, these studies did not focus on providing a unified, adaptive response for EV protection. Aldhyani et al. [3] and Chaganti et al. [8] explored deep learning models for securing various IoT contexts, offering insights that could be adapted for a more comprehensive EV defense system.

2.3 Decision Tree-Based and Other Novel Solutions

Yang et al. [23] developed a Decision Tree-based IDS for autonomous and networked vehicles, targeting both internal and external vehicle network intrusions. This approach, while valuable, lacks the guided and adaptive elements that GUARDEV proposes. Alamleh et al. [2] proposed a framework for standardizing ML-based IDSs in complex network settings, emphasizing the need for efficient

evaluation - a principle that aligns with GUARDEV's unified approach. Verma et al. [21] investigated specific attack vectors, underscoring the importance of a comprehensive defense strategy like GUARDEV.

3 GUARDEV: Proposed Framework

Our research introduces GUARDEV (Guided Unified Adaptive Response for Defending Electric Vehicles), a novel Intrusion Detection System (IDS) framework designed to secure Electric Vehicles (EVs) against various network threats. GUARDEV employs an ensemble stacking approach based on conflict resolution, integrating machine learning capabilities on the Internet of Vehicles (IoV) server. This framework leverages three advanced ML algorithms: Extreme Gradient Boosting (XGBoost) [17], Random Forest Classifier [9], and Extra Trees Classifier [18]. These algorithms work in concert to analyze IoV-based EV traffic data, creating a balanced, accurate, and adaptive intrusion detection model. The system architecture of GUARDEV is depicted in Fig. 2.

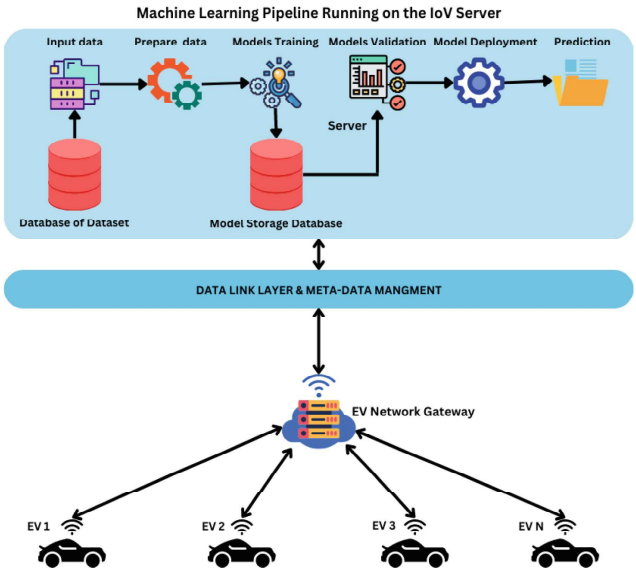


Fig. 2. GUARDEV System Architecture

GUARDEV's architecture is designed to provide a guided response to detected threats, unifying various security measures into a cohesive defence strategy. The adaptive nature of the system allows it to evolve with emerging threats, continuously improving its detection and response capabilities.

3.1 Dataset Description

To train and evaluate GUARDEV, we utilized the CICIoT2023 [16] dataset. This comprehensive dataset is crucial for developing machine learning models

capable of effectively detecting and responding to cyberattacks in IoV environments. The CICIoT2023 [16] dataset was meticulously curated by its authors, who collected data from 33 distinct cyberattacks conducted on a network comprising 105 IoT devices. These attacks span seven categories, encompassing threats highly relevant to EV security: DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, and Mirai. The dataset is publicly available, facilitating its use in training GUARDEV's machine learning algorithms to detect, classify, and guide responses to cyberattacks. By leveraging this rich dataset, GUARDEV can develop a nuanced understanding of various attack patterns, enabling it to provide guided, unified, and adaptive responses to protect EVs in real-world scenarios. The diversity of attack types represented in the dataset ensures that GUARDEV can offer comprehensive protection against a wide range of cyber threats in the IoV ecosystem.

3.2 Foundation ML Models for GUARDEV

GUARDEV incorporates three robust ML algorithms, each contributing to its guided, unified, and adaptive response capabilities:

- **Extreme Gradient Boosting (XGBoost):** XGBoost [17] forms a critical component of GUARDEV's adaptive response mechanism. It minimizes a regularized objective function:

$$\text{Obj}(\Theta) = \sum_i L(y_i, \hat{y}i^{(t)}) + \sum k\Omega(f_k), \tag{1}$$

  where $\hat{y}_i^{(t)}$ is the prediction at the t-th iteration, and f_k represents the k-th tree [10].
  Loss function: XGBoost typically uses logistic loss for binary classification:

$$L(y_i, \hat{y}_i) = y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i) \tag{2}$$

- **Random Forest (RF):** RF [9] contributes to GUARDEV's unified approach by creating an ensemble of decision trees:

$$RF(x) = \frac{1}{K} \sum_{k=1}^{K} h(x, \Theta_k), \tag{3}$$

  where K is the number of trees and Θ_k are the random parameters for the k-th tree [9].
  Loss function: RF typically uses Gini impurity for classification:

$$G = \sum_{i=1}^{c} p_i(1 - p_i) \tag{4}$$

  where c is the number of classes and p_i is the probability of an item being classified to class i.

– **Extra Trees (ET):** ET enhances GUARDEV's guided response by introducing controlled randomness:

$$ET(x) = \frac{1}{K} \sum_{k=1}^{K} h(x, \Theta_k, \theta_{best}), \tag{5}$$

where $\theta_{best} = \arg\max_{\theta} Q(D_v, \theta)$ [18].
Loss function: ET also typically uses Gini impurity, similar to Random Forest.

These algorithms were chosen for their complementary strengths in analytics, automated feature selection, low computational cost, and support for parallelization and GPU execution. Their integration in GUARDEV creates a versatile and efficient stacked-based ensemble model capable of providing a guided, unified, and adaptive response to cyber threats in Electric Vehicles. XGBoost's adaptive nature allows GUARDEV to continuously refine its response strategies. Random Forest contributes to the unified approach by aggregating multiple decision trees, providing robust predictions across various attack scenarios. Extra Trees introduce an element of controlled randomness, enhancing GUARDEV's ability to guide responses in novel threat situations. The combination of these algorithms enables GUARDEV to:

– Guide responses based on the strengths of each algorithm.
– Unify diverse prediction strategies for comprehensive threat detection.
– Adapt to evolving cyber threats in the Internet-connected EV ecosystem

The proposed model algorithm for GUARDEV is outlined in Algorithm 1, which details how these base models are integrated to create a cohesive, adaptive defense system for Electric Vehicles.

3.3 GUARDEV: A Stacked Ensemble Model for Guided, Unified, and Adaptive EV Cyber Defense

GUARDEV employs a sophisticated stacked ensemble comprising XGBoost [17], Random Forest [9], and Extra Trees [18] to enhance accuracy in identifying and responding to network attacks. Our approach integrates these diverse machine learning algorithms, leveraging each model's strengths to capture intricate patterns in network data and provide a guided, unified, and adaptive response. GUARDEV's stacking methodology aggregates predictions from multiple base models via a meta-learner, enabling adaptability to dynamic threat landscapes. The ensemble model demonstrates superior resilience, accuracy, and adaptability, making GUARDEV well-suited for real-world deployment in safeguarding critical EV infrastructure. This is supported by a detailed algorithmic overview, elucidating steps from data preprocessing to final decision-making and response generation.

GUARDEV Algorithm Overview: The core of GUARDEV is encapsulated in Algorithm 1, which outlines the comprehensive steps for providing a guided, unified, and adaptive response to cyber threats in electric vehicles, underpinned by intricate mathematical operations.

Mathematical Formulations of GUARDEV: GUARDEV's algorithm is underpinned by rigorous mathematical formulations that enable its guided, unified, and adaptive response to cyber threats in electric vehicles. Here, we present these formulations along with their relevance to GUARDEV's key features. *Data Transformation and Normalization:* The preprocessing phase employs the SMOTE algorithm for class balancing, creating synthetic samples (D_{balanced}) through interpolation:

$$D_{\text{balanced}}(x) = x + \lambda \cdot (x_{\text{nn}} - x), \quad \lambda \sim \text{Uniform}(0, 1), \tag{6}$$

where x_{nn} is a nearest neighbor of (x). This is followed by PCA for dimensionality reduction:

$$D_{\text{reduced}} = W^T \cdot D_{\text{std}}, \quad W = \arg\max \text{Var}(W^T \cdot D_{\text{std}}). \tag{7}$$

These transformations ensure that GUARDEV's base models work with balanced, normalized data, enhancing the system's adaptive capabilities.
Ensemble Learning and Model Evaluation: The ensemble learning process involves training each base learner on the transformed dataset. The accuracy (A_m) for each model is calculated using k-fold cross-validation. The ensemble's decision-making employs a weighted voting mechanism:

$$P_{\text{ensemble},x} = \arg\max_c \sum_{m \in M} w_m \cdot \mathbb{I}[P_{m,x} = c], \tag{8}$$

where w_m is the weight assigned to model m, and $\mathbb{I}[\cdot]$ is an indicator function. This unified approach ensures all models contribute to the defence strategy.
Guided Model Selection and Confidence Scoring: For each threat type (t), GUARDEV selects the most appropriate model:

$$M_t = \arg\max_{m \in M} A_m(t) \tag{9}$$

The confidence score for each prediction is calculated as:

$$C_{m,x} = \frac{\exp(f_m(x)c)}{\sum i \exp(f_m(x)_i)} \tag{10}$$

where $f_m(x)_c$ is the model's output for class (). This guided selection and confidence scoring enable targeted responses to specific threat types.
Adaptive Conflict Resolution and Decision Making: When model predictions differ, GUARDEV employs an adaptive conflict resolution algorithm. The final prediction and response are determined based on Bayesian updating of confidence scores:

$$P_{\text{final},x}, R_x = \text{GuideAdaptiveResponse}(P_{m,x}, C_{m,x} m \in M, M_t) \tag{11}$$

Algorithm 1 GUARDEV: Guided Unified Adaptive Response for Defending Electric Vehicles

Require: Dataset D with EV network traffic data, Set of ML models M = XGBoost, Random Forest, Extra Trees

Ensure: Guided, unified, and adaptive intrusion detection and response for each data sample

Data Preprocessing and Adaptation:
Apply SMOTE: $D_{\text{balanced}} \leftarrow \text{SMOTE}(D)$
Standardize features: $D_{\text{std}} \leftarrow \text{StandardScaler}(D_{\text{balanced}})$
Apply PCA: $D_{\text{reduced}} \leftarrow \text{PCA}(D_{\text{std}})$
Training Unified Base Learners:
for each model $m \in M$ **do**
    Train m on D_{reduced}
    Perform k-fold cross-validation
    $A_m \leftarrow \text{ComputeAccuracy}(m, D_{\text{reduced}})$
Guided Model Selection for Each Threat Type:
for each threat type t in D **do**
    $M_t \leftarrow \arg\max_{m \in M} A_m(t)$
    if tie in M_t **then**
        Choose model with minimum response time
Adaptive Prediction Phase:
for each sample x in D_{test} **do**
    for each model $m \in M$ **do**
        $P_{m,x} \leftarrow \text{Predict}(m, x)$
        $C_{m,x} \leftarrow \text{Confidence}(m, x)$
Unified Consensus and Guided Conflict Resolution:
for each sample x in D_{test} **do**
    if all $P_{m,x}$ are equal **then**
        Accept prediction $P_{m,x}$
    else
        $P_x, R_x \leftarrow \text{GuideAdaptiveResponse}(P_{m,x}, C_{m,x}, M_t)$
Final Guided Decision Making:
$D_{\text{responses}} \leftarrow \bigcup_{x \in D_{\text{test}}} (P_x, R_x)$
Adaptive Complexity Analysis:
$O(DFC)$, with D as dataset volume, F as number of features, and C as complexity of adaptive models
Continuous Learning and Adaptation:
Update model weights based on performance: $W_m \leftarrow \text{UpdateWeights}(M, D_{\text{responses}})$

where

$$P_{\text{final},x} = \arg\max_{c} \prod_{m \in M} P(c | P_{m,x}, C_{m,x}), \tag{12}$$

and $P(c|P_{m,x}, C_{m,x})$ is the posterior probability of class c given the model's prediction and confidence score. The response R_x is generated based on this final prediction and the specific threat type.

Table 1. Performance Comparison of GUARDEV with State-of-the-Art Models Across Key Metrics

Model	Accuracy (%)	AUC (%)	Recall (%)	Prec. (%)	F1 (%)	Model Training Time (s)
LSTM [6]	90.50	88.12	86.99	91.00	88.00	916.65
Random Forest Classifier [19]	81.25	79.47	78.35	80.56	79.77	198.8800
XGBoost [10]	76.80	74.89	75.59	77.59	76.60	230.5565
Extra Trees [18]	68.30	67.48	69.75	70.86	69.87	216.3456
Decision Tree Classifier [15]	60.45	59.62	58.17	60.66	60.64	170.4275
K Neighbors Classifier [19]	52.70	54.88	53.26	52.65	52.77	94.8725
Deep Convolutional Neural Network [20]	92.50	90.93	91.84	91.84	92.91	894.79
Quadratic Discriminant Analysis [12]	88.85	73.14	44.54	79.45	83.83	6.6650
SVM [4]	50.35	48.45	47.20	52.34	49.11	355.9950
GUARDEV	**99.47**	**98.65**	**97.77**	**99.10**	**98.86**	**185.4773**

Continuous Learning and Adaptation GUARDEV's adaptive mechanism is reinforced through continuous learning:

$$W_m \leftarrow \text{UpdateWeights}(M, D_{\text{responses}}) \tag{13}$$

where the model weights are updated based on their performance on recent threats, ensuring GUARDEV evolves with the threat landscape.
Complexity Analysis: The overall complexity of GUARDEV is $O(DFC)$, where D is the dataset volume, F is the number of features, and C encapsulates the complexity of the underlying models. This analysis ensures GUARDEV's scalability in real-world EV scenarios.

These mathematical formulations provide a rigorous foundation for GUARDEV's behaviour and performance characteristics. By integrating ensemble learning with sophisticated mathematical techniques, GUARDEV offers a guided, unified, and adaptive solution for intrusion detection in IoV-based EV networks.

4 Results and Discussion: GUARDEV's Performance in Defending Electric Vehicles

This section presents a comprehensive analysis of the experimental results obtained from the evaluation of GUARDEV (Guided Unified Adaptive Response for Defending Electric Vehicles). The performance of our model is compared against several state-of-the-art models using the CICIoT2023 [16] dataset, underpinning its superiority in accurately detecting and responding to a wide array of network attacks targeting electric vehicles. Table 2 shows the Area Under the Curve (AUC) per Attack Category for GUARDEV, showcasing its robust performance across various attack categories relevant to EV security. Impressively, the overall AUC is recorded at 0.99, as depicted in Table 1. In the subsequent section, we provide a detailed discussion of the findings presented in Table 2 and Table 1, elucidating the efficacy and significance of GUARDEV in providing a guided, unified, and adaptive response to cyber threats in the EV ecosystem.

4.1 GUARDEV's Accuracy and Adaptive Robustness in EV Defense

As demonstrated in Table 1 and Table 2, GUARDEV exhibits exceptional accuracy and adaptive robustness in detecting and responding to various network attacks targeting electric vehicles, surpassing several other models including Random Forest [9], Extra Trees [18], and XGBoost [17]. In the detection and

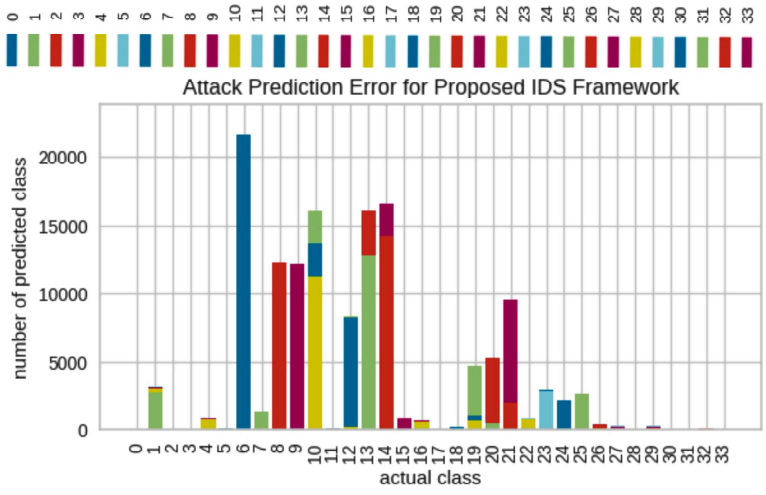


Fig. 3. Number of Attack Prediction Errors by the Proposed IDS Framework

response to 33 overall attack types relevant to EV security, GUARDEV achieved a remarkable accuracy of 99.47%. This showcases a significant improvement over:

- Random Forest [9]: 81.25% accuracy
- Extra Trees[18]: 68.30% accuracy
- XGBoost [17]: 76.80% accuracy

4.2 GUARDEV's Attack Prediction Error Analysis for Electric Vehicle Security

The performance of GUARDEV (Guided Unified Adaptive Response for Defending Electric Vehicles) was analyzed by examining the number of attack prediction errors across different attack classes relevant to EV security, as depicted by colors with corresponding numbers in Fig. 3. The graph illustrates the distribution of prediction errors made by GUARDEV. The x-axis represents the actual class of the attack, while the y-axis indicates the number of times GUARDEV incorrectly predicted the class of the attack. It is observed that GUARDEV made the highest number of errors on attacks belonging to classes 10, 11, and 12. This suggests that these particular attack classes may pose greater challenges in terms of detection in the EV ecosystem, possibly due to their complexity or GUARDEV's

Table 2. Category-Wise Area Under the Curve (AUC) Evaluation for GUARDEV Across Different Attack Vectors

Attack Category	Attack Sub-Category	AUC (Probability)
DDoS	ACK Fragmentation	0.99
DDoS	UDP Flood	1.00
DDoS	SlowLoris	0.99
DDoS	ICMP Flood	0.98
DDoS	RSTFIN Flood	1.00
DDoS	PSHACK Flood	0.99
DDoS	HTTP Flood	1.00
DDoS	UDP Fragmentation	1.00
DDoS	TCP Flood	1.00
DDoS	SYN Flood	1.00
DDoS	SynonymousIP Flood	0.98
Brute Force	Dictionary Brute Force	1.00
Spoofing	Arp Spoofing	0.99
Spoofing	DNS Spoofing	0.99
DoS	TCP Flood	0.99
DoS	HTTP Flood	1.00
DoS	SYN Flood	1.00
DoS	UDP Flood	0.99
Recon	Ping Sweep	0.98
Recon	OS Scan	0.98
Recon	Vulnerability Scan	0.99
Recon	Port Scan	1.00
Recon	Host Discovery	1.00
Web-based	SQL Injection	1.00
Web-based	Command Injection	1.00
Web-based	Backdoor Malware	1.00
Web-based	Uploading Attack	0.99
Web-based	XSS	0.98
Web-based	Browser Hijacking	0.99
Mirai	GREIP Flood	0.89
Mirai	Greeth Flood	1.00
Mirai	UDPPlain	0.87

limited training on such EV-specific attacks. Despite these errors, GUARDEV demonstrates overall effectiveness in detecting and responding to various attacks targeting electric vehicles. Understanding the nature of these errors is crucial for enhancing GUARDEV's adaptive capabilities and mitigating potential vulnerabilities in EV security.

4.3 Cumulative Gain Curve Analysis for GUARDEV's EV Protection Efficiency

The Cumulative Gain (CG) curve [14], depicted in Figure 4, stems from the evaluation of GUARDEV on a dataset of attack samples targeting electric vehicles. Each sample is categorized into specific attack classes denoted as C_i for $i = 1, 2, ..., N$, representing various cyber threats to EVs. Throughout the evaluation, attacks are sequentially analyzed, and the number of true positives (TPs) and false positives (FPs) for each class are recorded at every step, reflecting GUARDEV's guided and adaptive response capabilities.

Mathematically, at a particular step n, $TP_i(n)$ represents the number of correctly classified attacks belonging to class C_i. The cumulative gain at this step, denoted as $CG(n)$, is computed as:

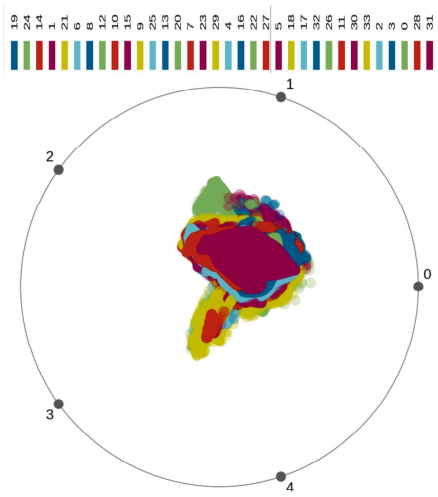


Fig. 4. Cumulative Gain Analysis of GUARDEV for Enhanced EV Cyber Defense

$$CG(n) = \frac{1}{N} \sum_{i=1}^{N} \frac{TP_i(n)}{T_i} \tag{14}$$

where T_i is the total number of attacks in class C_i, and N is the total number of attack classes relevant to EV security. The curve's concavity offers insights into GUARDEV's detection and response efficiency in the context of EV protection:

- **Concave-up Curve:** Indicates that GUARDEV prioritizes high-confidence attack detection, achieving significant initial gains in CG. This suggests that GUARDEV's guided response mechanism is particularly effective in quickly identifying and responding to the most prevalent or easily detectable EV-related cyber threats.
- **Plateaus:** Suggest saturation points where additional analysis yields diminishing returns, implying encounters with more challenging EV-specific attacks later in the analysis. These plateaus help identify areas where GUARDEV's adaptive mechanisms may need further refinement to address complex or evolving threats to electric vehicles.

The analysis of the CG curve furnishes valuable insights into GUARDEV's detection and response efficiency, aiding in the comprehensive assessment of its performance across various attack classes targeting EVs. This analysis is crucial for:

- Fine-tuning GUARDEV's guided response mechanisms for different types of EV-related cyber threats.
- Enhancing the unified approach to address a wider range of attack patterns specific to electric vehicles.
- Improving GUARDEV's adaptive capabilities to evolve with new and emerging threats in the EV ecosystem.

By leveraging these insights, GUARDEV can continually improve its ability to provide a comprehensive, efficient, and adaptive defence strategy for electric vehicles against the ever-evolving landscape of cyber threats.

5 Conclusion

Our study presents GUARDEV, a pioneering Guided Unified Adaptive Response framework for Defending Electric Vehicles within the Internet of Vehicles (IoV) ecosystem. By leveraging an ensemble-based machine learning (ML) approach that synergizes XGBoost, Random Forest, and Extra Trees, GUARDEV effectively mitigates diverse cyber threats prevalent in IoV environments. With an outstanding accuracy of 99.47% on the CICIoT2023 dataset, GUARDEV surpasses existing ML-based Intrusion Detection Systems (IDS) in both accuracy and F1-scores, showcasing its robustness and efficacy in safeguarding IoV networks against a spectrum of cyber threats. The comprehensive evaluation and analysis presented in this paper highlight the superiority of GUARDEV over state-of-the-art models. Notably, our framework demonstrates exceptional accuracy and robustness in detecting various network attacks, outperforming individual models such as Random Forest, Extra Trees, and XGBoost. The guided and adaptive nature of GUARDEV allows it to continuously refine its defence strategies, ensuring optimal protection against evolving threats. Furthermore, the detailed examination of attack prediction errors and the analysis of the Cumulative Gain curve provide valuable insights into GUARDEV's performance and areas for improvement. These insights inform the framework's adaptive capabilities, enabling it to enhance its defense mechanisms over time.

In conclusion, GUARDEV represents a significant advancement in EV cybersecurity within the IoV paradigm by addressing the pressing need for enhanced cybersecurity measures in IoV networks through a guided, unified, and adaptive solution. However, several hard research challenges remain, including the continuous adaptation of the framework to emerging, sophisticated cyber threats, integration of real-time data processing capabilities while maintaining high accuracy and low latency, and ensuring scalability to accommodate the growing number of connected vehicles and the increasing complexity of IoV networks. Future research should focus on developing more robust methods for real-time threat detection and response, exploring the integration of quantum computing techniques for enhanced cryptographic security, and investigating the ethical implications of autonomous decision-making in cybersecurity. Addressing these challenges will pave the way for even safer and more secure EV operations in the evolving landscape of connected vehicles and smart transportation systems, providing a robust and flexible defense mechanism capable of adapting to new and emerging cyber threats.

Acknowledgement. This work is partially supported by the DST IIT Bhilai Innovation and Technology Foundation (IBITF) under the grant IBITF/Note/EIR-PRAYAS/Cohort-03/SanctionLetter/2024-25/0076. We would like to express our grat-

itude to the foundation for their invaluable support and funding, which has significantly contributed to the successful completion of this research.

References

1. Agrawal, K., Alladi, T., Agrawal, A., Chamola, V., Benslimane, A.: Novelads: A novel anomaly detection system for intra-vehicular networks. IEEE Trans. Intell. Transp. Syst. **23**(11), 22596–22606 (2022)
2. Alamleh, A., Albahri, O., Zaidan, A., Albahri, A., Alamoodi, A., Zaidan, B., Qahtan, S., Alsatar, H., Al-Samarraay, M.S., Jasim, A.N.: Federated learning for iomt applications: A standardization and benchmarking framework of intrusion detection systems. IEEE J. Biomed. Health Inform. **27**(2), 878–887 (2022)
3. Aldhyani, T.H., Alkahtani, H.: Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. Mathematics **11**(1), 233 (2023)
4. Alshammari, A., Zohdy, M.A., Debnath, D., Corser, G.: Classification approach for intrusion detection in vehicle systems. Wirel. Eng. Technol. **9**(4), 79–94 (2018)
5. Arthurs, P., Gillam, L., Krause, P., Wang, N., Halder, K., Mouzakitis, A.: A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles. IEEE Trans. Intell. Transp. Syst. **23**(7), 6206–6221 (2022)
6. Ashraf, J., Bakhshi, A.D., Moustafa, N., Khurshid, H., Javed, A., Beheshti, A.: Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems. IEEE Trans. Intell. Transp. Syst. **22**(7), 4507–4518 (2020)
7. Awajan, A.: A novel deep learning-based intrusion detection system for iot networks. Computers **12**(2), 34 (2023)
8. Chaganti, R., Suliman, W., Ravi, V., Dua, A.: Deep learning approach for sdn-enabled intrusion detection system in iot networks. Information **14**(1), 41 (2023)
9. Chen, D., Yongchareon, S., Lai, E.M., Sheng, Q.Z., Liesaputra, V.: Locally weighted ensemble-detection-based adaptive random forest classifier for sensor-based online activity recognition for multiple residents. IEEE Internet Things J. **9**(15), 13077–13085 (2022)
10. Chen, T., Guestrin, C.: Xgboost: A scalable tree boosting system. In: Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining. pp. 785–794 (2016)
11. Chen, Z., Simsek, M., Kantarci, B., Djukic, P.: All predict wisest decides: A novel ensemble method to detect intrusive traffic in iot networks. In: 2021 IEEE Global Communications Conference (GLOBECOM). pp. 01–06. IEEE (2021)
12. Deolindo, V.M., Dalmazo, B.L., da Silva, M.V., de Oliveira, L.R., Silva, A.d.B., Granville, L.Z., Gaspary, L.P., Nobre, J.C.: Using quadratic discriminant analysis by intrusion detection systems for port scan and slowloris attack classification. In: International Conference on Computational Science and Its Applications. pp. 188–200. Springer (2021)
13. Elmasry, W., Akbulut, A., Zaim, A.H.: Evolving deep learning architectures for network intrusion detection using a double pso metaheuristic. Comput. Netw. **168**, 107042 (2020)
14. Huang, S., Poursafaei, F., Danovitch, J., Fey, M., Hu, W., Rossi, E., Leskovec, J., Bronstein, M., Rabusseau, G., Rabbany, R.: Temporal graph benchmark for machine learning on temporal graphs. Advances in Neural Information Processing Systems **36** (2024)

15. Ingre, B., Yadav, A., Soni, A.K.: Decision tree based intrusion detection system for nsl-kdd dataset. In: International conference on information and communication technology for intelligent systems. pp. 207–218. Springer (2017)
16. Neto, E.C.P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., Ghorbani, A.A.: Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment (2023)
17. Otchere, D.A., Ganat, T.O.A., Nta, V., Brantson, E.T., Sharma, T.: Data analytics and bayesian optimised extreme gradient boosting approach to estimate cut-offs from wireline logs for net reservoir and pay classification. Appl. Soft Comput. **120**, 108680 (2022)
18. Patel, A.M., Suthar, A.: Adaboosted extra trees classifier for object-based multispectral image classification of urban fringe area. Int. J. Image Graph. **22**(3), 2140006:1–2140006:16 (2022)
19. Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp **1**, 108–116 (2018)
20. Song, H.M., Woo, J., Kim, H.K.: In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications **21**, 100198 (2020)
21. Verma, A., Ranga, V.: Cosec-rpl: detection of copycat attacks in rpl based 6lowpans using outlier analysis. Telecommun. Syst. **75**, 43–61 (2020)
22. Wang, C., Li, Z., Xia, X., Shi, J., Si, J., Zou, Y.: Physical layer security enhancement using artificial noise in cellular vehicle-to-everything (C-V2X) networks. IEEE Trans. Veh. Technol. **69**(12), 15253–15268 (2020)
23. Yang, L., Moubayed, A., Hamieh, I., Shami, A.: Tree-based intelligent intrusion detection system in internet of vehicles. In: 2019 IEEE global communications conference (GLOBECOM). pp. 1–6. IEEE (2019)