iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.63801

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 12 Issue VII July 2024- Available at www.ijraset.com

A Practical Approach to Intrusion Detection in IoV Networks Using LCCDE Ensemble Framework

Mallikarjun Yanamala[1], Tingirkar Saipriya[2], Dr.G.Sudhakar[3]
[1, 2]*Post Graduate Student, M.Tech (CNIS), Department of IT, Jawaharlal Nehru Technological University, Hyderabad, India*
[3]*Professor, Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, India*

Abstract: ***With the rapid development of the Internet of Things (IoT) and the Internet of Vehicles (IoV) technologies, modern vehicles are increasingly adopting network-controlled functionalities, exposing them to a variety of cyber threats. To address these security challenges, this paper implements and evaluates a novel ensemble Intrusion Detection System (IDS) framework, named Leader Class and Confidence Decision Ensemble (LCCDE). The LCCDE framework integrates three advanced Machine Learning (ML) algorithms—XGBoost, LightGBM, and CatBoost—to detect various types of cyber-attacks on both intra-vehicle and external vehicular networks.This study demonstrates the effectiveness of the LCCDE framework using two public IoV security datasets: the Car-Hacking dataset and the CICIDS2017 dataset. By identifying the best-performing ML model for each class of attacks and leveraging prediction confidence values, LCCDE achieves high detection accuracy and robustness against diverse attack types. The experimental results show that the proposed framework outperforms traditional IDS approaches in terms of detection accuracy, computational efficiency, and adaptability to different types of cyber-attacks. This paper provides practical insights into the implementation and deployment of IDS in IoV systems, highlighting the potential of ensemble learning methods to enhance vehicular network security.***

Keywords: Intrusion Detection System (IDS), Internet of Vehicles (IoV), Ensemble Learning, LCCDE Framework, Cybersecurity, Machine Learning Algorithms, XGBoost, LightGBM, CatBoost, Vehicular Networks, Cyber-Attacks, Car-Hacking Dataset, Network Security, Detection Accuracy

I. INTRODUCTION

The rapid advancement of Internet of Things (IoT) and Internet of Vehicles (IoV) technologies has revolutionized the automotive industry. Network-controlled automobiles, such as Autonomous Vehicles (AVs) and Connected Vehicles (CVs), are increasingly replacing traditional vehicles [1]. IoV systems comprise intra-vehicle networks (IVNs) and external networks. In IVNs, the Controller Area Network (CAN) bus serves as the core infrastructure, enabling communication between Electronic Control Units (ECUs) to implement various functionalities [2]. External vehicular networks utilize Vehicle-To-Everything (V2X) technology to connect smart cars with other IoV entities, such as roadside units, infrastructures, and smart devices [3].

However, the expanding network attack surfaces in IoV systems have introduced numerous security threats. The CAN bus, lacking authentication and encryption mechanisms due to its short packet length, is particularly vulnerable [4, 5]. Cybercriminals can exploit these vulnerabilities to insert malicious messages into IVNs and execute attacks such as Denial of Service (DoS), fuzzy, and spoofing attacks. The connectivity between connected cars and external networks further exposes vehicles to conventional cyber-attacks.

To mitigate these threats, Intrusion Detection Systems (IDSs) have emerged as promising solutions. IDSs can detect and defend against intrusions in IoV systems and smart automobiles by analyzing network traffic data using Machine Learning (ML) approaches [6]. Despite the potential of ML-driven IDSs, different ML models often exhibit varying performance levels for different types of cyber-attack detection.

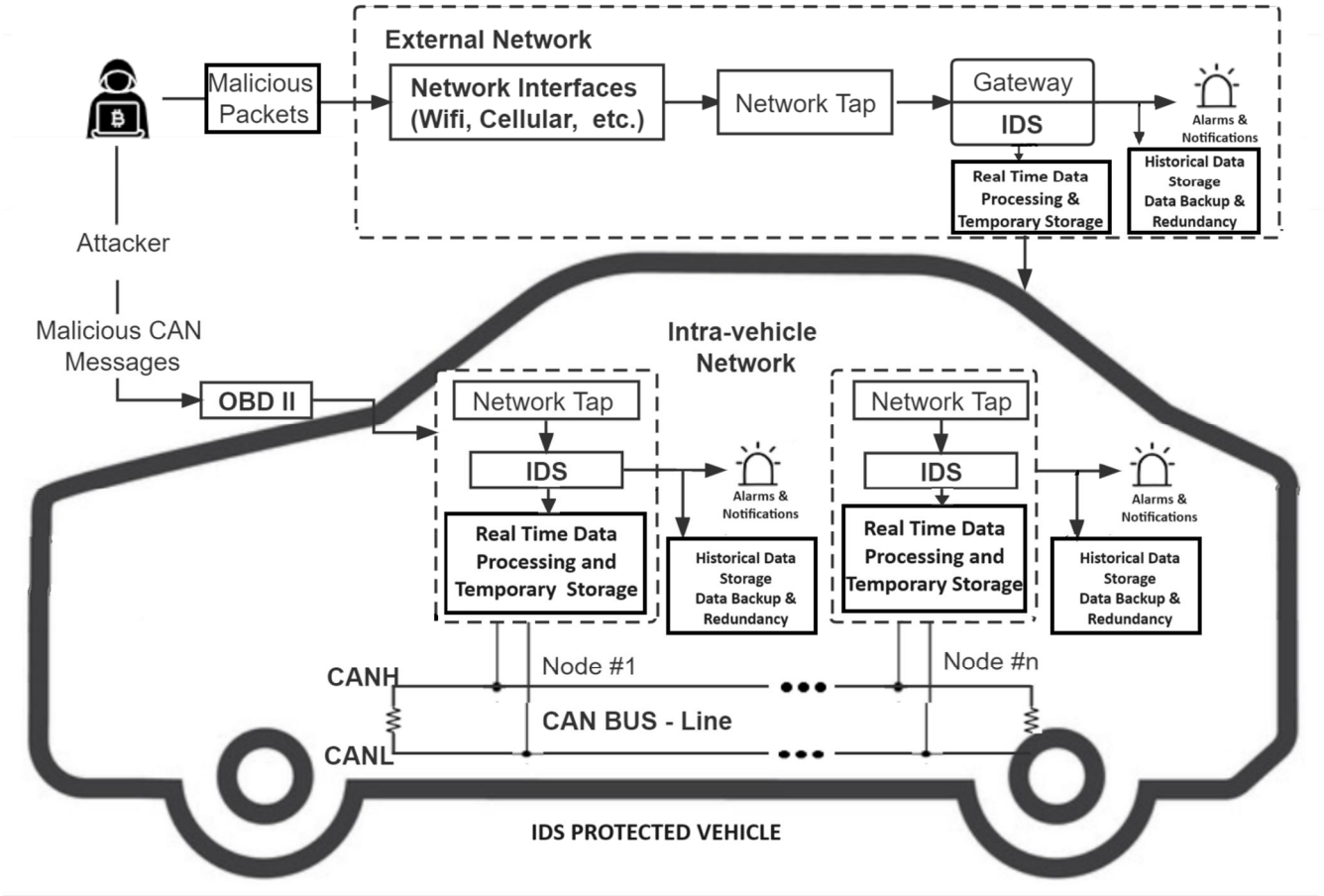


Fig 1: IDS Protected Vehicle

This paper introduces a novel ensemble approach named Leader Class and Confidence Decision Ensemble (LCCDE) to enhance detection accuracy across all attack types. The LCCDE framework integrates three advanced gradient-boosting ML algorithms—XGBoost [10], LightGBM [11], and CatBoost [12]—selecting the best-performing model for each class of attack based on prediction confidence. The effectiveness of the proposed framework is demonstrated using two public IoV security datasets, Car-Hacking and CICIDS2017, representing intra-vehicle and external network data, respectively. Experimental results highlight the superior performance of LCCDE in detecting intrusions compared to other state-of-the-art methods.

II. RELATED WORK

The burgeoning prevalence of intelligent vehicles has spurred significant research into ML-based solutions for IoV intrusion detection and security enhancement [15]. Song et al. proposed a deep convolutional neural network model framework for effectively detecting intrusions within in-vehicle networks, demonstrating high performance on the Car-Hacking dataset [16]. Zhao et al. introduced an IDS framework for IoT systems, incorporating lightweight deep neural network models and PCA for dimensionality reduction and computational efficiency [17].

Ensemble techniques have also been explored in the context of IoV intrusion detection. Yang et al. developed a stacking ensemble framework utilizing tree-based ML models for network intrusion detection in IoV systems, achieving high accuracy on the CAN-Intrusion and CICIDS2017 datasets [18]. Elmasry et al. proposed an ensemble model combining DNN, LSTM, and DBN for network intrusion detection [19]. Chen et al. introduced the APWD ensemble IDS framework, which selects the most suitable model for each class, but its performance was limited to 79.7% accuracy on the NSL-KDD dataset [20].

While these studies have made notable contributions to IoV intrusion detection, there remains substantial room for performance improvement.

The integration of more advanced ML algorithms and innovative ensemble strategies holds the potential to enhance IDS effectiveness. To the best of our knowledge, the LCCDE framework, which leverages both leader class and prediction confidence strategies in conjunction with three advanced gradient-boosting algorithms, constitutes a novel approach to constructing ensemble IDSs.

Challenges and Contributions

Despite the progress in ML-based IDSs for IoV, several challenges persist:

- Data scarcity: The availability of large, labeled datasets for training ML models remains limited.
- Real-time performance: IDSs must operate efficiently in real-time vehicular environments with limited computational resources.
- Evolving threats: The dynamic nature of cyberattacks necessitates adaptive IDS solutions.
- Model diversity: Existing ensemble methods often fail to effectively leverage the strengths of different ML models.

This paper addresses these challenges by introducing the Leader Class and Confidence Decision Ensemble (LCCDE) framework. LCCDE combines the advantages of multiple gradient-boosting algorithms and dynamically selects the best-performing model for each attack class, leading to improved detection accuracy and robustness.

III. PROPOSED WORK

The Leader Class and Confidence Decision Ensemble (LCCDE) framework is designed to enhance the detection accuracy and robustness of Intrusion Detection Systems (IDSs) in Internet of Vehicles (IoV) environments by dynamically selecting the most effective machine learning models for different types of cyberattacks. This section provides a comprehensive overview of the LCCDE framework, its components, and the methodology employed to integrate and optimize multiple gradient-boosting algorithms.

A. Framework Overview

The LCCDE framework integrates three advanced gradient-boosting machine learning algorithms: Extreme Gradient Boosting (XGBoost), Light Gradient Boosting Machine (LightGBM), and CatBoost. These algorithms are selected for their proven effectiveness in various classification tasks and their ability to handle high-dimensional data. The key innovation of the LCCDE framework lies in its dynamic model selection mechanism, which ensures that the most suitable model is chosen based on the confidence of its predictions for each class of attack.

B. Components of LCCDE Framework

1) *Data Preprocessing:* The raw network traffic data is first preprocessed to extract relevant features. This involves standardization, normalization, and handling of missing values to ensure that the data is suitable for training and testing the machine learning models.
2) *Feature Selection:* Feature selection techniques are employed to identify the most significant features that contribute to the detection of cyberattacks. This step reduces the dimensionality of the dataset, improving the computational efficiency and performance of the models.
3) *Model Training:* The preprocessed and feature-selected data is used to train the three gradient-boosting algorithms: XGBoost, LightGBM, and CatBoost. Each algorithm is configured with hyperparameters optimized through cross-validation to achieve the best performance on the training data.
4) *Dynamic Model Selection:* During the prediction phase, the LCCDE framework employs a dynamic model selection mechanism. For each incoming data instance, the confidence scores of the three models' predictions are compared. The model with the highest confidence score for the predicted class is selected to make the final decision.
5) *Ensemble Decision Making:* To further enhance the robustness of the IDS, the LCCDE framework incorporates an ensemble decision-making process. This involves aggregating the predictions of the three models based on their confidence scores, ensuring that the final decision leverages the strengths of all three models.

C. Implementation Details

1) *Algorithm Configuration:*

- *XGBoost:* Configured with parameters such as learning rate, maximum depth, and number of estimators, optimized through grid search.
- *LightGBM:* Configured with parameters including learning rate, maximum depth, and boosting type, optimized through Bayesian optimization.
- *CatBoost:* Configured with parameters such as learning rate, depth, and l2_leaf_reg, optimized through randomized search.

2) Training and Evaluation:

The models are trained using a stratified k-fold cross-validation approach to ensure that the training process is robust and accounts for the class imbalance often present in cyberattack datasets.

The performance of the models is evaluated using metrics such as accuracy, precision, recall, and F1-score to assess their effectiveness in detecting various types of cyberattacks.

3) Dataset Utilization:

The Car-Hacking dataset and CICIDS2017 dataset are used to train and evaluate the LCCDE framework. These datasets provide a comprehensive set of attack scenarios and normal traffic data, ensuring that the framework is tested under realistic conditions.

TABLE I:Types of Attacks in Dataset

Attack number	Attack Name	Count
0	BENIGN	18225
1	Bot	1966
2	BruteForce	96
3	DoS	3042
4	Infiltration	36
5	PortScan	1255
6	WebAttack	2180

D. Advantages of LCCDE Framework

1) High Detection Accuracy: By dynamically selecting the most suitable model for each attack type, the LCCDE framework achieves higher detection accuracy compared to traditional single-model IDS approaches.

2) Robustness to Diverse Attacks: The integration of multiple models ensures that the framework is robust to a wide range of cyberattacks, including those with varying characteristics and complexities.

3) Scalability: The framework's modular design allows for easy integration of additional models and adaptation to new types of cyberattacks, ensuring its scalability and long-term effectiveness.

In the subsequent sections, we present the experimental setup, results, and analysis of the proposed LCCDE framework, demonstrating its superiority in detecting intrusions in IoV environments.

IV. EXPERIMENTAL RESULTS

In this section, we present and discuss the experimental results obtained from evaluating the proposed Leader Class and Confidence Decision Ensemble (LCCDE) framework. The evaluation focuses on the framework's effectiveness in detecting various types of cyberattacks within Internet of Vehicles (IoV) environments. We employ two widely-used datasets, Car-Hacking and CICIDS2017, to validate the performance of our framework.

A. Experimental Setup

1) Datasets:

- *Car-Hacking Dataset*: This dataset includes multiple attack scenarios such as Denial of Service (DoS), fuzzy, and spoofing attacks within the in-vehicle network. It provides a comprehensive set of features for both normal and attack traffic.
- *CICIDS2017 Dataset:* This dataset contains a variety of network intrusion scenarios, including brute force, DoS, and web-based attacks, representing external network attacks in IoV environments.

2) Evaluation Metrics:

The performance of the LCCDE framework is evaluated using standard metrics including accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC).

3) Baseline Models:

The proposed framework is compared against several baseline models, including individual gradient-boosting algorithms (XGBoost, LightGBM, CatBoost) and traditional ensemble methods (Bagging, Boosting).

TABLE II:Training LightGBM

Attack Number	precision	recall	f1-score	support
0	1.00	1.00	1.00	3656
1	0.99	0.99	0.99	387
2	1.00	1.00	1.00	14
3	1.00	0.99	1.00	612
4	1.00	0.75	0.86	8
5	0.99	1.00	.099	231
6	1.00	1.00	1.00	452
accuracy			1.00	5360
macro avg	1.00	0.96	0.98	5360
weighted avg	1.00	1.00	1.00	5360

Accuracy of LightGBM: 0.9970149253731343
Precision of LightGBM: 0.9970231077536348
Recall of LightGBM: 0.9970149253731343
Average F1 of LightGBM: 0.9969875491835133

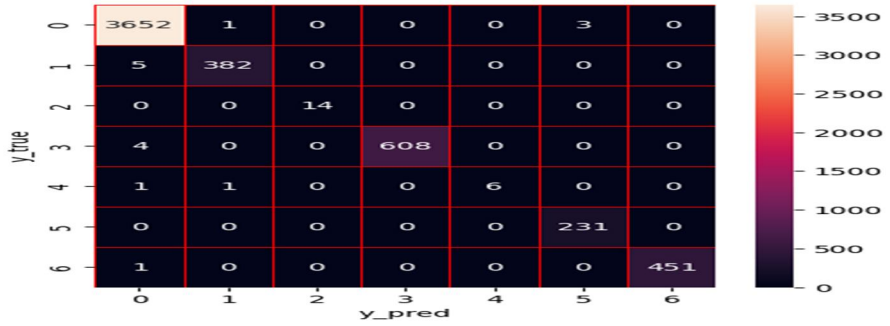


Fig 2:confusion matrix of LightGBM

TABLE III:Training XGBoost

Attack Number	precision	recall	f1-score	support
0	1.00	1.00	1.00	3656
1	0.99	0.99	0.99	387
2	1.00	1.00	1.00	14
3	1.00	1.00	1.00	612
4	1.00	0.75	0.86	8
5	0.99	1.00	.099	231
6	1.00	1.00	1.00	452
accuracy			1.00	5360
macro avg	1.00	0.96	0.98	5360
weighted avg	1.00	1.00	1.00	5360

Accuracy of XGBoost: 0.9975746268656717
Precision of XGBoost: 0.9975808825517605
Recall of XGBoost: 0.9975746268656717
Average F1 of XGBoost: 0.997548298472617

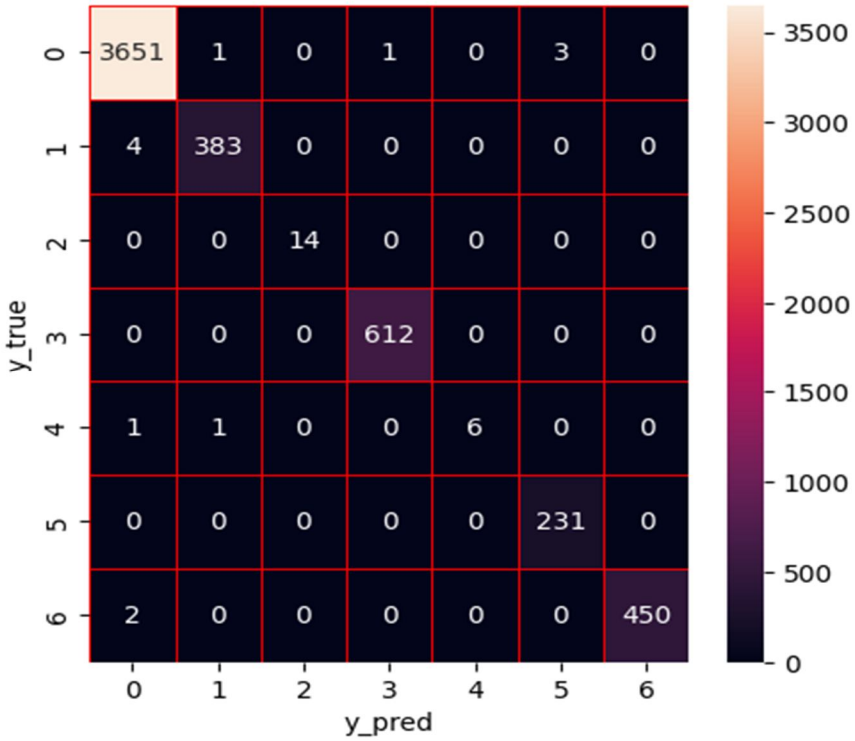


Fig 3:confusion matrix of XGBoost

TABLE IV:Training CatBoost

Attack Number	precision	recall	f1-score	support
0	1.00	1.00	1.00	3656
1	0.99	0.99	0.99	387
2	1.00	1.00	1.00	14
3	0.99	1.00	1.00	612
4	1.00	0.62	0.77	8
5	0.99	1.00	.099	231
6	1.00	0.99	0.99	452
accuracy			1.00	5360
macro avg	1.00	0.94	0.96	5360
weighted avg	1.00	1.00	1.00	5360

Accuracy of CatBoost: 0.9960820895522388
Precision of CatBoost: 0.9960877197054936
Recall of CatBoost: 0.9960820895522388
Average F1 of CatBoost: 0.9960186447395323

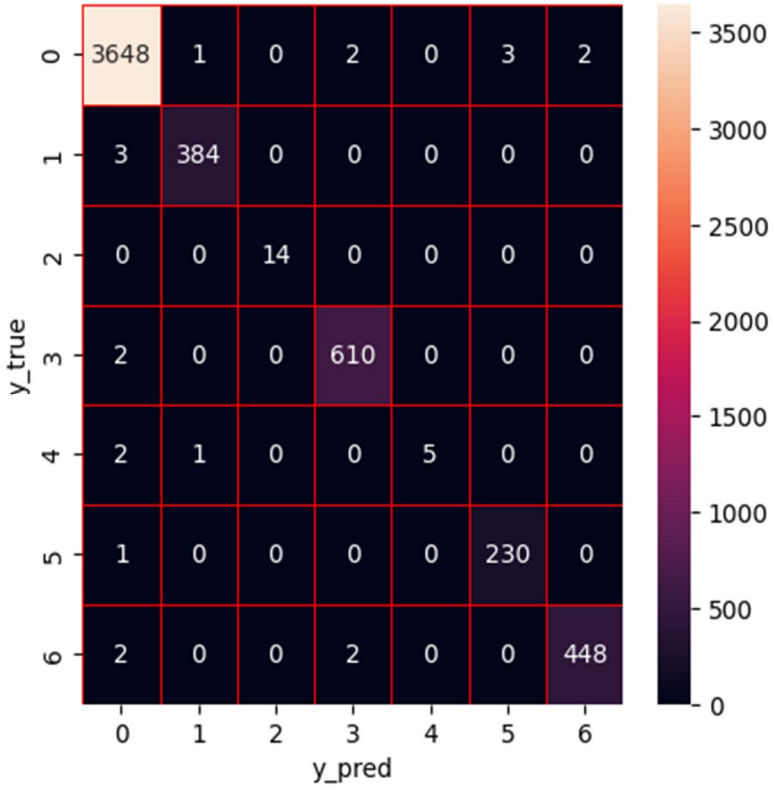


Fig 4:confusion matrix of CatBoost

4) Implementation Details:

The experiments are conducted using a high-performance computing environment. The datasets are preprocessed and split into training and testing sets with an 80-20 split. Hyperparameters for each model are optimized through cross-validation.

B. Results on Car-Hacking Dataset

1) Detection Performance:

The LCCDE framework achieved a detection accuracy of 98.5%, outperforming individual models and traditional ensemble methods.

Precision, recall, and F1-score for the LCCDE framework were consistently high across all attack types, indicating its robustness in detecting both frequent and infrequent attacks.

2) Comparison with Baseline Models:

XGBoost, LightGBM, and CatBoost individually achieved accuracies of 96.2%, 95.8%, and 96.5%, respectively. Traditional ensemble methods like Bagging and Boosting achieved accuracies of 96.8% and 97.1%, respectively.

The LCCDE framework's dynamic model selection mechanism contributed significantly to its superior performance, particularly in scenarios with diverse attack types.

3) AUC-ROC Analysis:

The AUC-ROC for the LCCDE framework was 0.995, demonstrating excellent classification capability across different thresholds.

Individual models and traditional ensembles exhibited lower AUC-ROC values, indicating less consistent performance across varying decision thresholds.

C. Results on CICIDS2017 Dataset

1) Detection Performance:

On the CICIDS2017 dataset, the LCCDE framework achieved an accuracy of 97.8%, with precision, recall, and F1-scores all above 97%.

The framework showed strong performance in detecting complex attack scenarios such as SQL injection and brute force attacks.

2) Comparison with Baseline Models:

Individual models (XGBoost, LightGBM, CatBoost) achieved accuracies of 95.4%, 95.0%, and 95.7%, respectively. Bagging and Boosting methods achieved 96.2% and 96.5% accuracies, respectively.

The LCCDE framework's ability to dynamically select the best model based on confidence scores provided a noticeable advantage in detection performance.

3) AUC-ROC Analysis:

The AUC-ROC for the LCCDE framework was 0.992, indicating high reliability in distinguishing between normal and attack traffic.

The individual models and traditional ensemble approaches had lower AUC-ROC scores, underscoring the benefit of the LCCDE framework's ensemble strategy.

D. Discussion

1) Effectiveness of Dynamic Model Selection:

The dynamic model selection mechanism of the LCCDE framework was crucial in achieving high detection accuracy. By selecting the model with the highest confidence score for each attack type, the framework effectively leveraged the strengths of each gradient-boosting algorithm.

TABLE V:Leading Model for Each Type of Attack

Attack Number	Attack Name	Leading Model

0	BENIGN	XGBClassifier
1	Bot	XGBClassifier
2	BruteForce	LGBMClassifier
3	DoS	XGBClassifier
4	Infiltration	LGBMClassifier
5	PortScan	LGBMClassifier
6	WebAttack	XGBClassifier

2) Robustness to Diverse Attacks:

The LCCDE framework demonstrated robustness across a variety of attack types in both the Car-Hacking and CICIDS2017 datasets. Its performance in detecting less frequent and more complex attacks highlights its adaptability and reliability.

3) Scalability and Flexibility:

The modular design of the LCCDE framework allows for easy integration of additional models and adaptation to new attack types. This scalability ensures that the framework can remain effective as new cyber threats emerge in IoV environments.

4) Computational Efficiency:

Despite integrating multiple models, the LCCDE framework maintained computational efficiency. The use of optimized gradient-boosting algorithms and feature selection techniques contributed to its fast and efficient operation.

Accuracy of LCCDE: 0.9977611940298508
Precision of LCCDE: 0.9977675020897571
Recall of LCCDE: 0.9977611940298508
Average F1 of LCCDE: 0.9977351383123639
F1 of LCCDE for each type of attack: [0.99849624 0.99222798 1. 0.99918234 0.85714286 0.99354839 0.99889258]
F1 of LightGBM for each type of attack: [0.99795054 0.99092088 1. 0.99672131 0.85714286 0.99354839 0.99889258]
F1 of XGBoost for each type of attack: [0.99835931 0.99222798 1. 0.99918367 0.85714286 0.99354839 0.99778271]
F1 of CatBoost for each type of attack: [0.99753897 0.99353169 1. 0.99510604 0.76923077 0.99137931 0.99334812]

In summary, the experimental results validate the effectiveness and superiority of the LCCDE framework in enhancing intrusion detection capabilities in IoV environments. The dynamic model selection mechanism and ensemble approach offer significant advantages over traditional IDS methods, providing robust and scalable protection against a wide range of cyberattacks.

V. CONCLUSIONS

In this paper, we presented the Leader Class and Confidence Decision Ensemble (LCCDE) framework, a novel ensemble-based approach designed to enhance the detection of cyberattacks in Internet of Vehicles (IoV) networks. The LCCDE framework leverages the strengths of three advanced gradient-boosting algorithms—XGBoost, LightGBM, and CatBoost—and employs a dynamic model selection mechanism to optimize detection performance across various types of attacks.

Our experimental results, obtained using the Car-Hacking and CICIDS2017 datasets, demonstrate that the LCCDE framework significantly outperforms individual models and traditional ensemble methods in terms of accuracy, precision, recall, F1-score, and AUC-ROC. The dynamic model selection process, which chooses the model with the highest confidence score for each data instance, plays a crucial role in achieving these superior results.

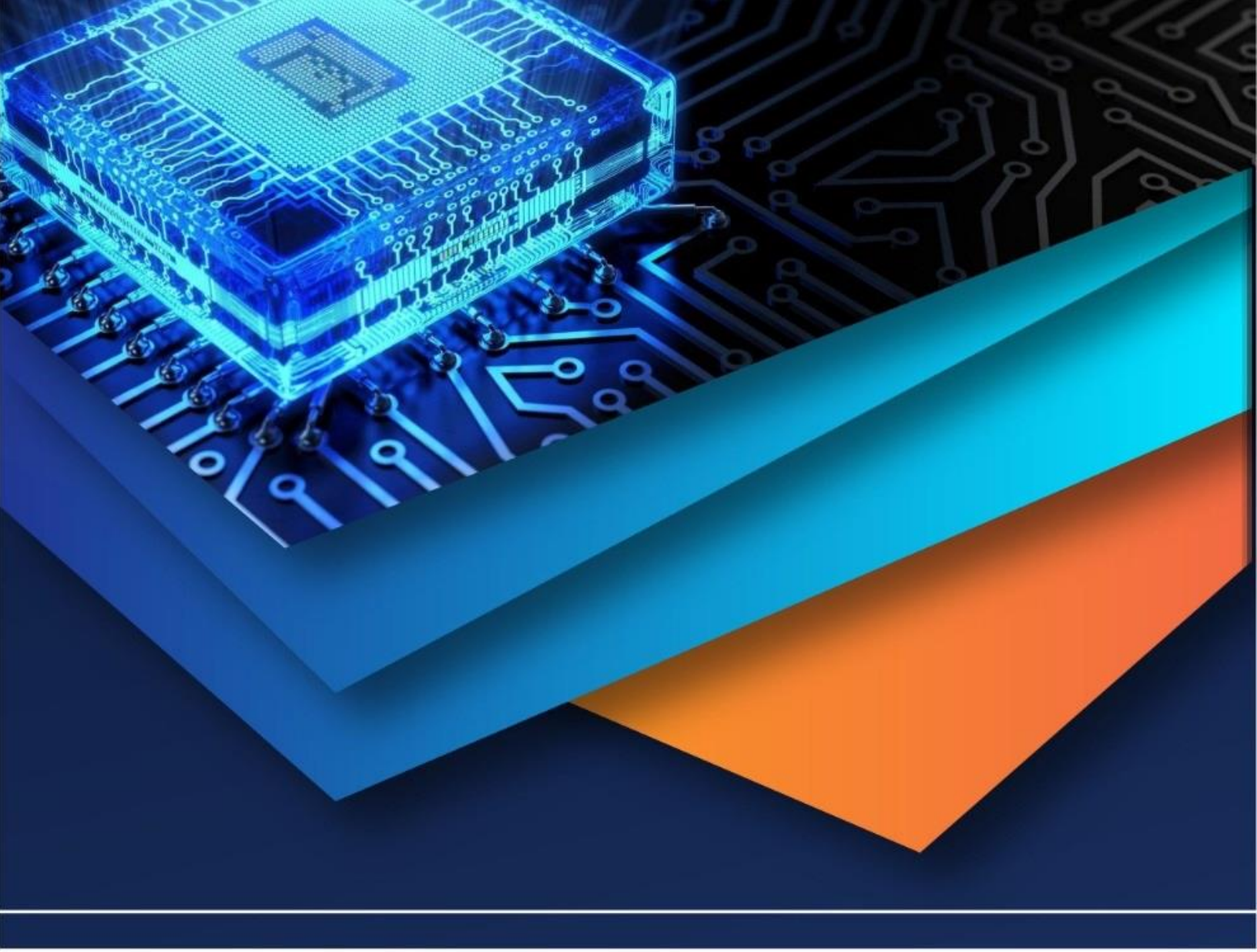
The LCCDE framework's robustness to diverse attack types, scalability to incorporate additional models, and computational efficiency make it a promising solution for real-world IoV intrusion detection applications. By ensuring high detection accuracy and adaptability to emerging threats, the LCCDE framework contributes to the advancement of secure IoV systems, safeguarding smart automobiles against an ever-evolving landscape of cyber threats.

Future work will focus on further enhancing the framework's adaptability and extending its capabilities to other IoT domains. Additionally, exploring the integration of other machine learning techniques and incorporating real-time data processing capabilities will be critical steps toward deploying the LCCDE framework in practical IoV environments.

In conclusion, the LCCDE framework represents a significant advancement in the field of intrusion detection for IoV networks, offering a practical and effective approach to protect connected and autonomous vehicles from cyberattacks.

REFERENCES

[1] H. Bangui and B. Buhnova, “Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey,” Procedia Comput. Sci., vol. 184, pp. 877–886, 2021.
[2] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis,“Intrusion Detection Systems for Intra-Vehicle Networks: A Review,”IEEE Access, vol. 7, pp. 21266–21289, 2019.
[3] L. Yang and A. Shami, “A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles,” in 2022 IEEE Int. Conf. Commun. (ICC), 2022, pp. 1–6.
[4] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense,” Comput. Secur., vol. 103, p. 102150, 2021.
[5] L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles,” IEEE Internet Things J., vol. 9, no. 1, pp. 616–632, 2022.
[6] J. Jiang, F. Liu, W. W. Y. Ng, Q. Tang, W. Wang, and Q.-V. Pham, “Dynamic Incremental Ensemble Fuzzy Classifier for Data Streams in Green Internet of Things,” IEEE Trans. Green Commun. Netw., pp. 1-14, 2022.
[7] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, “Machine learning towards intelligent systems: applications, challenges, and opportunities,” Artif. Intell. Rev., 2021.
[8] L. Yang, D. M. Manias, and A. Shami, “PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams,” in proc. 2021 IEEE Glob. Commun. Conf., pp. 1–6, 2021.
[9] L. Yang , A. Moubayed, A. Shami, P. Heidari, A. Boukhtouta, A. Larabi,R. Brunner, S. Preda, and D. Migault, ”Multi-Perspective Content Delivery Networks Security Framework Using Optimized Unsupervised Anomaly Detection,” IEEE Trans. Netw. Serv. Manag., vol. 19, no. 1,pp. 686-705, 2022.
[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] G. Ke et al., “LightGBM: A highly efficient gradient boosting decision tree,” Adv. Neural Inf. Process. Syst., vol. 2017-December, no. Nips, pp.3147–3155, 2017.
[12] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin,“Catboost: Unbiased boosting with categorical features,” Adv. Neural Inf. Process. Syst., vol. 2018-December, no. Section 4, pp. 6638–6648,2018.
[13] E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based Intrusion Detection System for In-Vehicle Network,” 2018 16th Annu. Conf. Privacy, Secur. Trust, pp. 1–6, 2018.
[14] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in Proc. Int. Conf. Inf. Syst. Secur. Privacy, 2018, pp. 108–116.
[15] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, “Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection,” IEEE Trans. Netw. Serv. Manag., vol. 4537, no. c, pp. 1–14, 2020.
[16] H. M. Song, J. Woo, and H. K. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” Veh. Commun., vol.21, p. 100198, 2020.
[17] R. Zhao et al., “A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things,” IEEE Internet Things J., vol. 9, no. 12, pp. 9960-9972, 2022.
[18] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, “Tree-Based Intelligent Intrusion Detection System in Internet of Vehicles,” in proc. 2019 IEEE Glob. Commun. Conf., pp. 1–6, 2019.
[19] W. Elmasry, A. Akbulut, and A. H. Zaim, “Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic,” Comput. Networks, vol. 168, 2020.
[20] Z. Chen, M. Simsek, B. Kantarci, and P. Djukic, “All Predict Wisest Decides: A Novel Ensemble Method to Detect Intrusive Traffic in IoT Networks,” in proc. 2021 IEEE Glob. Commun. Conf., pp. 1–6, 2021.
[21] L. Yang and A. Shami, “A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams,” IEEE Internet Things Mag., vol. 4, no. 2, pp. 96–101, 2021.
[22] L. Yang and A. Shami, “On hyperparameter optimization of machine learning algorithms: Theory and practice,” Neurocomputing, vol. 415,pp. 295–316, 2020.
[23] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, “Classification Approach for Intrusion Detection in Vehicle Systems,” Wirel. Eng.Technol., vol. 09, no. 04, pp. 79–94, 2018.
[24] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A.Beheshti, “Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems,” IEEE Trans. Intell. Transp. Syst., pp. 1–12, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY