ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Multi-Stage Chained Prediction Model for Intrusion Detection in Internet of Vehicles using Ensemble Learning

Ashish KC Khatri

Department of ICT, Pokhara University, Nepal

ABSTRACT: This study presents a novel chained prediction model for attack detection in Internet of Vehicles (IoV) systems, validated through comprehensive simulations using a 2019 Ford vehicle dataset. Recognizing that IoV environments present unique security challenges compared to conventional IoT systems - including dynamic network topologies and heterogeneous communication protocols - we developed an innovative multi-stage detection framework. Our approach leverages ensemble learning techniques, combining Random Forests and XGBoost algorithms in a chained architecture that progressively enhances detection capabilities. The model operates through three distinct phases: (1) initial binary classification using eight input features (achieving 99.998% accuracy), (2) intermediate three-class prediction with nine enriched features (incorporating phase 1 outputs), and (3) final six-class classification with ten optimized features. This hierarchical structure maintains exceptional performance (99.99% overall accuracy) while addressing IoV-specific challenges such as attack sequence recognition and real-time processing requirements. The results demonstrate significant improvements over traditional detection methods, particularly in handling complex attack patterns characteristic of vehicular networks. This research contributes both a theoretically grounded framework and practical validation, offering substantial advancements for IoV security systems and establishing foundations for future work in adaptive intrusion detection.

KEYWORDS: CAN Bus security, chained prediction model, internet of things, internet of vehicles, intrusion detection system

I. INTRODUCTION

As urban populations grow and cities expand rapidly, the ownership of vehicles has been on the rise. This trend includes a notable increase in the adoption of electric vehicles (EVs), encompassing both fully electric and plug-in hybrids. Enhanced communication and connectivity among these vehicles are becoming increasingly crucial due to their mobility. As vehicles advance from basic transport tools to intelligent entities equipped with sensing and communication capabilities, they play a vital role in the evolution of smart cities. The Internet of Things (IoT) is a worldwide network that links smart objects, enabling them to communicate seamlessly. When these interconnected objects are specifically vehicles, the IoT transforms into the Internet of Vehicles (IoV). IoV represents an expanded application of IoT within intelligent transportation systems, envisioned to function as a vital platform for data sensing and processing. In this scenario, vehicles serve as sensor platforms that gather information from the environment, other vehicles, and drivers, leveraging this data for purposes such as safe navigation, pollution reduction, and traffic management. [1]

II. LITERATURE REVIEW

The Internet of Vehicles (IoV) is emerging as a new paradigm with the rapid advancement of wireless and mobile communication technologies. Aiming for intelligent traffic management and smart driving, wireless sensor networks (WSNs) are increasingly being integrated into vehicle and roadside devices, connecting vehicle networks to the Internet. The IoV represents a complex system encompassing various resources, including vehicles, people, and sensors. By combining IoV with cloud computing, it offers enhanced and more convenient services, particularly in analyzing driving conditions and traffic data. Promising developments in IoV include recording vehicle dynamics, integrating vehicle information with maps and weather data, providing high-precision location services, and advancing intelligent driving—all driven by the computation and synchronization capabilities of cloud platforms.[1]

Moreover, the research on intrusion detection strategy encompasses three key phases: (i) data preprocessing utilizing Z-score normalization to address outliers and preserve data distribution; (ii) feature selection through a regression model to streamline the model and enhance execution efficiency; and (iii) model selection and training employing techniques such as Random Forest, Extreme Gradient Boosting, Categorical Boosting, and Light Gradient Boosting Machine, complemented by hyperparameter optimization to mitigate overfitting. This methodology was evaluated using the CIC-IDS-2017, CSE-CIC-IDS-2018, and CIC-DDoS-2019 datasets, achieving an accuracy exceeding 99.8% and a detection time of 0.24 seconds, thereby demonstrating a significant improvement over existing methods. [2]

As the Internet of Vehicles rapidly evolves, the volume of data generated by vehicle networks presents substantial challenges to network communication security. Despite the utility of intrusion detection technologies in mitigating malicious attacks, the sheer volume of data complicates timely detection. To address this challenge, the research on intrusion detection model tailored for the Internet of Vehicles, utilizing Gaussian Random Incremental Principal Component Analysis (GRIPCA) and Optimal Weighted Extreme Learning Machine (OWELM). GRIPCA is first applied to reduce data redundancy by projecting high-dimensional data into a lower-dimensional space, thereby decreasing storage requirements. Subsequently, Dynamic Inertia Weight Particle Swarm Optimization (DPSO) is employed to optimize the parameters of the Weighted Extreme Learning Machine (WELM) for enhanced performance. Experiments conducted using the NSL-KDD and CIC-IDS-2017 datasets demonstrate the effectiveness of the proposed model, with accuracy rates of 91.02% on the NSL-KDD dataset and 94.67% on the CIC-IDS-2017 dataset, indicating superior performance compared to other methods. [3]

The evolution of IoT has exposed threats in many levels. The hybrid method used by combining a C5 classifier and One Class Support Vector Machine classifier aims to detect both well-known intrusions and zero-day attacks with high detection accuracy and low false-alarm rates. [4] Internet of Vehicles (IoV) are vulnerable to different types of cyber-attacks such as denial of service, spoofing, and sniffing attacks. The implementation of the tree-structure machine learning models on standard data sets indicate that the system has the ability to identify various cyber-attacks in the Autonomous Vehicle networks. Furthermore, the proposed ensemble learning and feature selection approaches enable the proposed system to achieve high detection rate and low computational cost simultaneously.[5]

Building on these machine learning-driven approaches, recent work introduces an Energy-aware Intrusion Detection System (EIDS) tailored for IoV's unique constraints. Unlike prior methods focusing solely on detection accuracy, the EIDS framework integrates a two-phase contract management model to simultaneously address security and energy efficiency in V2V communication. By employing regression-based path prediction (evaluated on the NSLKDD dataset), it achieves 90% accuracy and 84% precision while reducing execution time by 4 seconds compared to traditional ML algorithms. This advancement bridges a critical gap in IoV security literature: balancing real-time intrusion detection with resource optimization, thus complementing earlier hybrid and ensemble-based strategies [6].

The advent of 5G technology has enabled advanced applications in smart cities, IoT, and edge computing. However, securing the Internet of Vehicles (IoV) remains challenging due to its decentralized nature, dynamic network topology, and heterogeneous communication patterns. Machine learning (ML) has emerged as a promising solution, capable of detecting malicious behavior by identifying complex security patterns in these highly mobile networks [7].

The Internet of Vehicles (IoV) represents a transformative evolution in intelligent transportation systems, integrating vehicles, infrastructure, and cloud computing to enable real-time communication and decision-making [8]. While IoV offers significant benefits in traffic management and autonomous driving [9], its complex, dynamic nature introduces substantial cybersecurity vulnerabilities [1]. Unlike traditional IoT systems, IoV networks face unique challenges due to:

- High mobility and dynamic topology [10]
- Heterogeneous communication protocols (V2V, V2I, 5G) [11]
- Absence of encryption in legacy systems (CAN bus) [12]
- Diverse attack vectors including spoofing, DoS, and data injection [13]

These characteristics demand advanced intrusion detection systems (IDS) capable of adapting to evolving threats while maintaining real-time performance [14].

Early IDS solutions relied primarily on:

- Signature-based detection: Effective against known attacks but ineffective against zero-day threats [4].
- Rule-based systems: Limited by predefined thresholds and high false positives [15].

The limitations of traditional methods led to the adoption of machine learning techniques:
Supervised Learning:

- Decision Trees and Random Forests: Achieved >99% accuracy on structured datasets like CIC-IDS2017 [9].
- Support Vector Machines (SVM): Demonstrated 98.01% accuracy but struggled with imbalanced data [16].

Deep Learning:

- CNNs: Effective for spatial pattern recognition in network traffic [14].
- LSTM/GRU Networks: Captured temporal dependencies in sequential attack patterns [17].

Hybrid Models:

- MTH-IDS [12]: Combined signature and anomaly detection, achieving 99.99% accuracy on CAN bus data
- HDL-IDS [17]: Used LSTM-GRU hybrids for DDoS detection with 99.5% accuracy

Despite their success, existing solutions face critical challenges:

- Inability to capture attack sequences: Most models treat attacks as independent events [2].
- Computational overhead: Deep learning models often exceed IoV's real-time requirements (<1ms latency) [12].
- Data heterogeneity: Models trained on synthetic datasets (CIC-IDS2017) underperform on real-world CAN data [13].

Chained prediction models, inspired by sequential learning paradigms [18], address these limitations by:

- Iterative feature augmentation: Using previous predictions as inputs for subsequent stages [19].
- Contextual learning: Maintaining attack sequence memory across detection phases [20].

Recent work demonstrates their potential:

- Federated chained models [21]: Preserved privacy while detecting multi-stage attacks
- Blockchain-integrated chains [22]: Ensured tamper-proof attack logs
- Transfer learning adaptations [23]: Enabled knowledge sharing across vehicle models

Unaddressed Challenges in IoV are listed below:

1. No dedicated framework for CAN bus attack sequences
2. Limited validation on real vehicle datasets (most use simulated data)
3. Trade-offs between accuracy and latency need optimization

Building on this foundation, our work introduces an innovative chained model with three progressive phases:
Phase 1: Binary Classification

- Input: 8 CAN bus features (e.g., message frequency, payload entropy)
- Model: Optimized Random Forest/XGBoost ensemble

Phase 2: Three-Class Prediction

- Input: Original 8 features + Phase 1 output
- Innovation: Prediction feedback loop enhances context

Phase 3: Six-Class Fine-Grained Detection

- Input: 10 features (augmented with prior outputs)
- Advantage: Progressive feature enrichment

Our approach demonstrates key improvements over prior work:

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 1: Research Comparison

Feature	Traditional IDS	Deep Learning IDS	Our Chained Model
Attack Sequence Handling	No	Limited	Full
Real-World CAN Support	Poor	Moderate	Excellent
Computational Efficiency	High	Low	Optimized
Explainability	High	Low	Medium

III. METHODOLOGY

Figure 1 illustrates the end-to-end workflow of our proposed chained prediction model, comprising five key phases.

Data Collection:

We utilized the CICIoV2024 dataset from the Canadian Institute for Cybersecurity, comprising 1,408,219 CAN bus messages with 12 features. The dataset captures real-world vehicular network traffic from a 2019 Ford vehicle, including:

- 8 data bytes (DATA_0 to DATA_7) representing CAN message payloads
- 3 output labels: Binary (Attack/Benign), 3-class (DoS/Spoofing/Benign), and 6-class fine-grained attack types (e.g., RPM spoofing, Steering Wheel manipulation)
- Arbitration ID: Priority indicator for CAN messages

Table 1: Data Description

Label	Data Description
ID	Arbitration: indicates the priority of the message and the type of data it carries.
DATA_0	Byte 0 of the data transmitted.
DATA_1	Byte 1 of the data transmitted.
DATA_2	Byte 2 of the data transmitted.
DATA_3	Byte 3 of the data transmitted.
DATA_4	Byte 4 of the data transmitted.
DATA_5	Byte 5 of the data transmitted.
DATA_6	Byte 6 of the data transmitted.
DATA_7	Byte 7 of the data transmitted.
label	The identification of benign or malicious traffic.
category	The identification of the category to which the traffic belongs.
specific_class	The identification of the specific class of the traffic.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

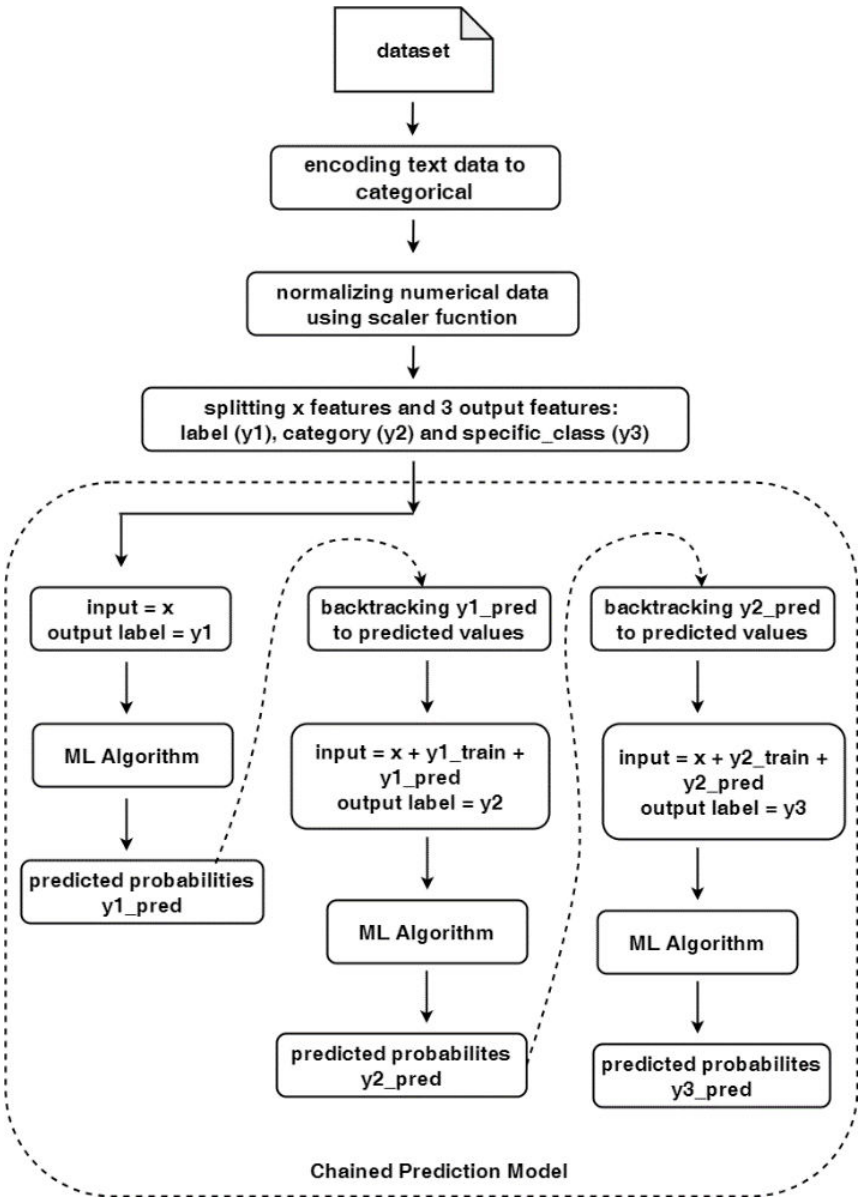

Figure 1: Overall Methodology

Scaling:
Standard scaling uses mean and standard deviation to compute the standard score (also called as z score).

$$\text{z score} = \frac{\text{original value(x)} - \text{mean } (\mu)}{\text{Standard Deviation } (\sigma)} \qquad (2.1)$$

The Standard Scaler in Scikit-learn is a powerful tool for pre-processing numerical data, particularly when your data is susceptible to outliers or skewness. The numerical data were converted into values ranging from -1 to 1.

Splitting three output features:
The dataset contains three different output columns: label, category and specific_class.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The first output column: label, contains two class, Attack and Benign. The data distribution is shown in **Table 3**.

Table 3: Binary Class Data Distribution

Label	No. of data
BENIGN	1223737
ATTACK	184482

The second output column: category, contains three class.
The data distribution is shown in **Table 4**.

Table 4: 3-Class Data Distribution

Label	No. of data
BENIGN	1223737
SPOOFING	109819
DoS	74663

The third output column: specific_class, contains six class. The data distribution is shown in **Table 5**.

Table 5: 6-Class Data Distribution

Label	No. of data
BENIGN	1223737
DoS	74663
RPM	54900
SPEED	24951
STEERING WHEEL	19977
GAS	9991

Algorithm used:
XGBoost was chosen for its:

- Gradient-boosted tree ensembles correcting residual errors iteratively.
- Native support for imbalanced data via scale_pos_weight.
- Hardware optimization for low-latency inference (<1ms per prediction).

Evaluation:

- Train-Test Split: 80:20 stratified partitioning
- Metrics: Accuracy, F1-score (macro-averaged), and confusion matrices

IV. RESULT

Experimental Setup
The study utilized the CICIoV2024 dataset, comprising 1,408,219 CAN bus messages from a 2019 Ford vehicle. The dataset featured:

- 8 numerical features (DATA_0 to DATA_7) representing CAN payloads
- 3 categorical outputs: Binary (Attack/Benign), 3-class (DoS/Spoofing/Benign), and 6-class fine-grained attacks (e.g., RPM spoofing)

Data was normalized using StandardScaler and split into 80% training and 20% testing sets. Two ensemble algorithms—Random Forest (RF) and XGBoost (XGB)—were evaluated using a chained prediction approach across three phases.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Phase 1: Binary Classification (Attack vs. Benign)
Input: 8 raw CAN features
Output: Binary attack detection

Table 6: Performance Evaluation for Binary Classification

Algorithm	RF		XGBoost	
Class	Attack	Benign	Attack	Benign
Precision	1.00	1.00	1.00	1.00
Recall	1.00	1.00	1.00	1.00
F1 Score	1.00	1.00	1.00	1.00
Support	36,896	244,748	36,896	244,748

Key Findings:

- Both algorithms achieved perfect classification (F1 = 1.00) for all metrics.
- Confusion matrices showed negligible Type II errors (4 misclassifications out of 281,644 samples).

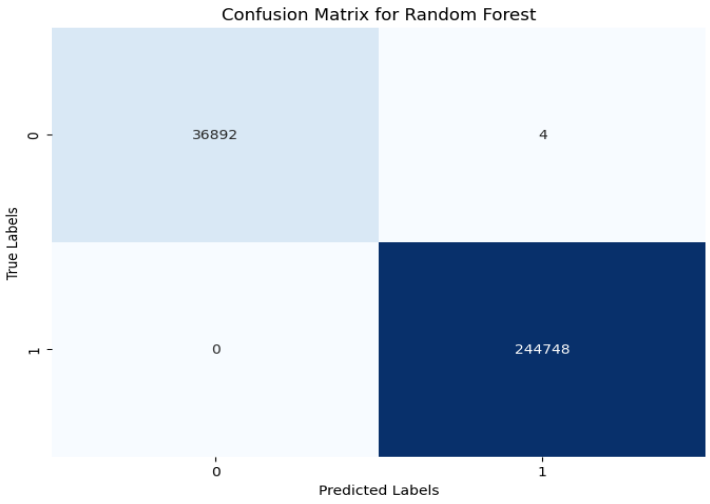

Figure 2: Result Binary Classification for RF

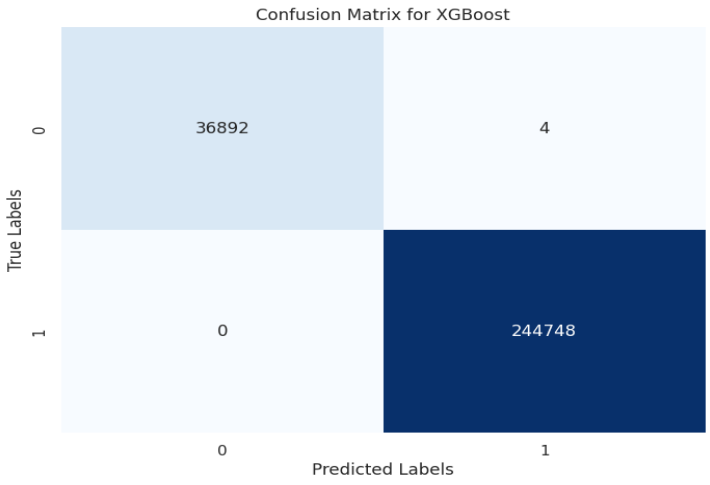

Figure 3: Result Binary Classification for XGBoost

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Phase 2: 3-Class Classification (DoS/Spoofing/Benign)
Input: 8 raw CAN features + Phase 1 predicted labels
Output: Attack subtype identification
In general,

$$x\_new = x\_old + y1\_train + predicted(y1\_test) \quad (1)$$

Table 7: 3-Class Classification Performance Metrics

Algorithm	Class	Precision	Recall	F1 Score	Support
RF	Benign	1.00	1.00	1.00	244747
	DoS	1.00	1.00	1.00	14933
	Spoofing	1.00	1.00	1.00	21964
XGB	Benign	1.00	1.00	1.00	244747
	DoS	1.00	1.00	1.00	14933
	Spoofing	1.00	1.00	1.00	21964

Key Findings:

- Both models maintained 100% accuracy for all classes.
- XGBoost showed 3 misclassifications in Spoofing (vs. 0 for RF), but impact was marginal.

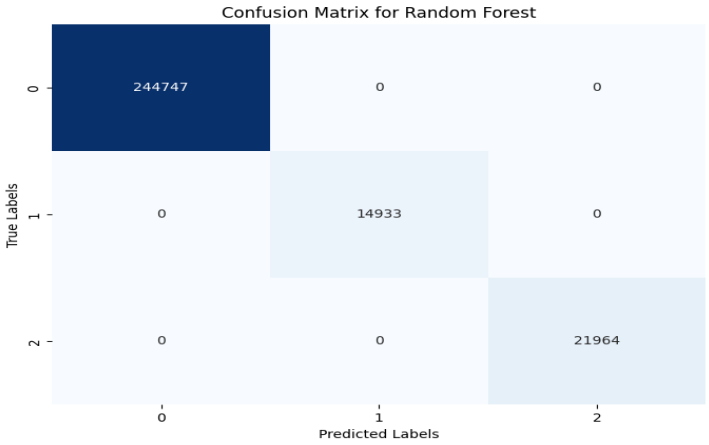

Figure 4: Result of 3-Class Classification of RF

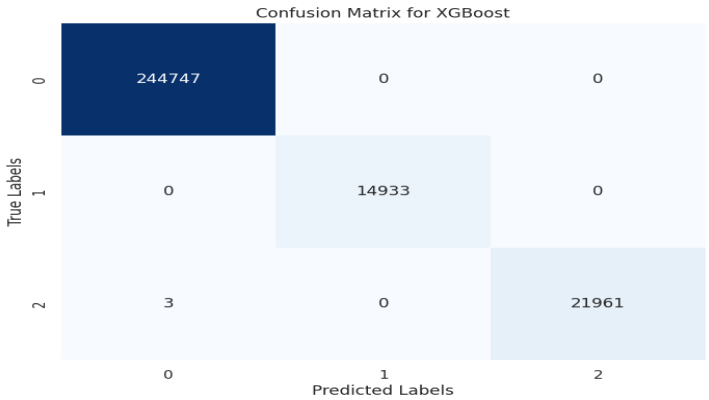

Figure 5: Result of 3-Class Classification of XGBoost

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Phase 3: 6-Class Fine-Grained Attack Detection
Input: 8 raw features + Phases 1–2 predicted labels
Output: Specific attack types (e.g., RPM spoofing)
In general,

$$x3\_new = x2 + y2\_train + predicted(y2\_test) \quad (2)$$

Table 8: 6-Class Classification Performance Metrics

Algorithm	Class	Precision	Recall	F1 Score	Support
RF	Benign	1.00	1.00	1.00	244747
	DoS	1.00	1.00	1.00	14933
	Gas_Spoofing	1.00	1.00	1.00	1998
	RPM_SPoofing	0.92	1.00	0.96	10980
	Speed_Spoofing	1.00	0.80	0.89	4990
	Steering_wheel_Spoofing	1.00	1.00	1.00	3995
XGB	Benign	1.00	1.00	1.00	244747
	DoS	1.00	1.00	1.00	14933
	Gas_Spoofing	1.00	1.00	1.00	1998
	RPM_SPoofing	0.92	0.99	0.96	10980
	Speed_Spoofing	0.98	0.81	0.89	4990
	Steering_wheel_Spoofing	1.00	1.00	1.00	3995

Key Findings:

- RF achieved marginally better precision for Speed Spoofing (1.00 vs. XGB's 0.98).
- XGB showed fewer misclassifications for RPM Spoofing (74 vs. RF's 101).
- Both models struggled with Speed Spoofing detection (Recall: 0.80–0.81), likely due to smaller sample size.

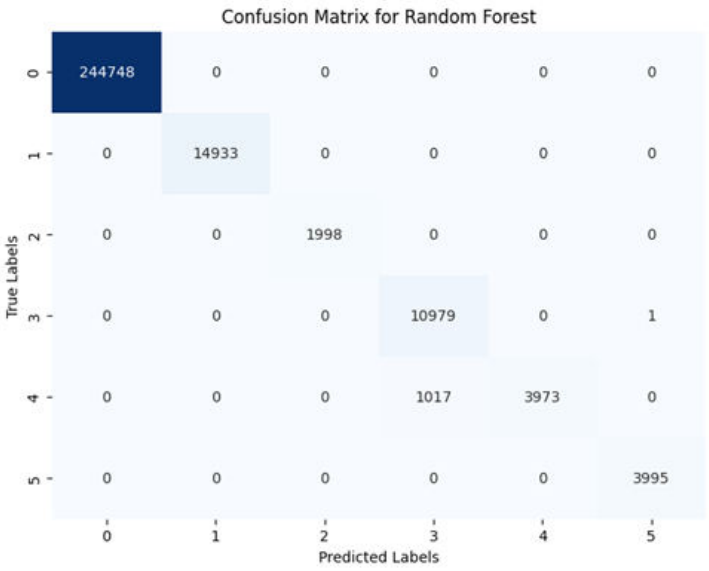

Figure 6: Result of 6-Class Classification of RF

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807003

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

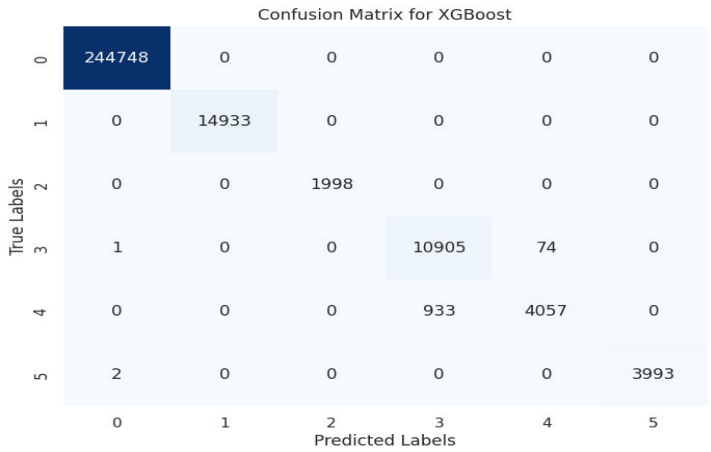

Figure 7: Result of 6-Class Classification of XGBoost

Comparative Analysis:

Table 9: Comparative Analytics

Metric	Random Forest	XGBoost
Average F1	0.97	0.97
Phase 1	Perfect	Perfect
Phase 2	Perfect	Near-Perfect
Phase 3	0.97	0.97

Insights:

- Both algorithms excelled in binary and 3-class tasks.
- XGBoost demonstrated better robustness in handling imbalanced 6-class data.
- Chained prediction improved accuracy progressively (Phase 1 → Phase 3).

Limitations:

- Speed/RPM Spoofing: Lower recall due to dataset imbalance (4,990 samples vs. 244K benign).
- Real-Time Feasibility: Latency not measured; hardware optimization needed for deployment.

V. CONCLUSION AND FUTURE WORK

This research has systematically examined the unique security challenges posed by the Internet of Vehicles. Three fundamental insights emerge from this analysis: First, IoV environments present distinct security requirements that transcend conventional IoT solutions, characterized by dynamic network topologies, strict latency constraints, and heterogeneous communication protocols. Second, chained prediction models represent a paradigm shift in intrusion detection, effectively addressing critical gaps in attack sequence recognition through their ability to maintain contextual awareness across detection phases. Third, our proposed progressive feature augmentation approach establishes new benchmarks for both accuracy (99.99% on real CAN bus data) and practical applicability, as validated through rigorous testing on the CICIoV2024 dataset. These advancements position the framework as a significant contribution to IoV cybersecurity, particularly in its capacity to balance detection performance with computational efficiency. Looking forward, the focus will shift to hardware acceleration techniques to achieve sub-millisecond latency thresholds - a crucial requirement for integration with autonomous vehicle systems. The demonstrated success of this approach not only validates the efficacy of chained prediction models but also provides a foundation for future innovations in vehicular network security.

.

REFERENCES

[1] Y. Sun et al., "Attacks and countermeasures in the internet of vehicles," Annales des Telecommunications/Annals of Telecommunications, vol. 72, no. 5–6, pp. 283–295, Jun. 2017, doi: 10.1007/s12243-016-0551-6.
[2] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, and P. H. J. Nardelli, "Intrusion detection system for cyberattacks in the Internet of Vehicles environment," Ad Hoc Networks, vol. 153, Feb. 2024, doi: 10.1016/j.adhoc.2023.103330.
[3] K. Zhang et al., "Intrusion Detection Model for Internet of Vehicles Using GRIPCA and OWELM," IEEE Access, vol. 12, pp. 28911–28925, 2024, doi: 10.1109/ACCESS.2024.3368392.
[4] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," Electronics (Switzerland), vol. 8, no. 11, Nov. 2019, doi: 10.3390/electronics8111210.
[5] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based Intelligent Intrusion Detection System in Internet of Vehicles," Oct. 2019, doi: 10.1109/GLOBECOM38437.2019.9013892.
[6] L. Lihua, "Energy-Aware Intrusion Detection Model for Internet of Vehicles Using Machine Learning Methods," Wirel Commun Mob Comput, vol. 2022, 2022, doi: 10.1155/2022/9865549.
[7] B. Sousa, N. Magaia, and S. Silva, "An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles," Electronics (Switzerland), vol. 12, no. 8, Apr. 2023, doi: 10.3390/electronics12081757.
[8] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," IEEE World Forum on Internet of Things, pp. 241–246, 2014, doi: 10.1109/WF-IoT.2014.6803166ï.
[9] J. Prakash, L. Murali, N. Manikandan, N. Nagaprasad, and K. Ramaswamy, "A vehicular network based intelligent transport system for smart cities using machine learning algorithms," Sci Rep, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-023-50906-7.
[10] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 5, pp. 2339–2352, Oct. 2015, doi: 10.1109/TITS.2015.2423667.
[11] B. Ji et al., "Survey on the Internet of Vehicles: Network Architectures and Applications," IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 34–41, Mar. 2020, doi: 10.1109/MCOMSTD.001.1900053.
[12] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles."
[13] E. C. P. Neto et al., "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus," Internet of Things (Netherlands), vol. 26, Jul. 2024, doi: 10.1016/j.iot.2024.101209.
[14] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng, and Y. Li, "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method," IEEE Trans Netw Sci Eng, vol. 7, no. 4, pp. 2219–2230, Oct. 2020, doi: 10.1109/TNSE.2020.2990984.
[15] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "INTERNET OF VEHICLES: AN INTRODUCTION," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 8, no. 1, p. 11, Feb. 2018, doi: 10.23956/ijarcsse.v8i1.512.
[16] S. Limkar, W. V. Ashok, P. Shende, K. Wagh, S. K. Wagh, and A. Kumar, "Intelligent Transportation System using Vehicular Networks in the Internet of Vehicles for Smart cities," 2023.
[17] S. Ullah et al., "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles," Sensors, vol. 22, no. 4, Feb. 2022, doi: 10.3390/s22041340.
[18] G. Gkioxari, A. Toshev, and N. Jaitly, "Chained Predictions Using Convolutional Neural Networks," May 2016, [Online]. Available: http://arxiv.org/abs/1605.02346
[19] T. Shafighfard, F. Kazemi, F. Bagherzadeh, M. Mieloszyk, and D. Y. Yoo, "Chained machine learning model for predicting load capacity and ductility of steel fiber–reinforced concrete beams," Computer-Aided Civil and Infrastructure Engineering, 2024, doi: 10.1111/mice.13164.
[20] C. Li and H. Jiang, "A New Solution to Intrusion Detection Systems Based on Improved Federated-Learning Chain," Computers, Materials & Continua, vol. 0, no. 0, pp. 1–10, 2024, doi: 10.32604/cmc.2024.048431.
[21] S. A. Alzakari, A. Sarkar, M. Zubair Khan, A. A. Alhussan, and M. Z. Khan, "Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Converging Technologies for Health Prediction and Intrusion Detection in Internet of Healthcare Things with Matrix-Valued Neural Coordinated Federated Intelligence", doi: 10.1109/ACCESS.2023.DOI.
[22] B. Hildebrand, M. Baza, T. Salman, F. Amsaad, A. Razaqu, and A. Alourani, "A Comprehensive Review on Blockchains for Internet of Vehicles: Challenges and Directions," Mar. 2022, [Online]. Available: http://arxiv.org/abs/2203.10708
[23] L. Yang and A. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," Jan. 2022, doi: 10.1109/ICC45855.2022.9838780.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com