Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

REAL-TIME THREAT DETECTION IN CONNECTED CARS: A MACHINE LEARNING APPROACH TO MITM ATTACKS

[1]Adnan, [2]Daud Khan, [3]Junaid Ur Rahman, [4]Mohd Sumer, [5]Hamad Bashir Ahmad

[1]*European University Of Lefke Turkish Republic Of Northern Cyprus Mersin Turkiye*
[2]*Iqra National University*
[3]*University of Roehampton, London*
[4]*University of Roehampton, London*
[5]*Iqra National University*

DOI: https://doi.org/10.5281/zenodo.20066288

Keywords
Support Vector Machine; K-Nearest Neighbors; Man-in-the-Middle

Article History
Received on 14 April, 2026
Accepted on 05 May, 2026
Published on 07 May, 2026

Corresponding Author: *

Abstract

This research investigates how several machine learning (ML) models are trained and evaluated to identify different forms of Man-in-the-Middle (MitM) attacks in connected cars. The framework integrated incorporates continuous surveillance and live threat identification to improve security of vehicles. The four machine learning algorithms, which include Decision Tree Classifier, Logistic Regression, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN), were deployed and evaluated in the CARLA simulation world. Several attack scenarios, spoofing attacks, Denial-of-Service (DoS) attacks, and replay attacks were included in the simulation to the vehicle control unit. The results show that the Decision Tree Classifier had the best threat detection accuracy of 97.50, and the precision, recall, and F1-scores were consistent across all types of attacks. Also, the K-Nearest Neighbors model had a 90.00% accuracy, which shows that it is competitive in terms of threat detection. The results revealed the efficiency of machine learning-based solutions in terms of securing connected vehicles with the help of real-time monitoring and efficient attack detection systems.

Introduction

A self-driving vehicle is a type of autonomous vehicle that can drive itself without any human input—based on the report of the autonomous vehicle market which represents a researcher by Allied Market Research, the level of the global market value was estimated to be $54.23 bn in 2019, on the fair condition predicted to increase to $556.67 bn in 2026, which developing with the compound growth rate of 39.47% from 2019 to 2026. Most of the world's population - 57 percent - have heard of autonomous vehicles, and want to use them. Today, the market of autonomous vehicles is worth $54 billion. The German brand Audi intends to invest $16 billion in the business through 2023. Are ports predicting that there will be 33 million AVs on the road by 2040? Globally, 80+ companies are about testing 1400+ self-driving vehicles (Sadaf et al., 2023).

In automotive automation, driving will be automated, without the driver controlling or monitoring the vehicle and surroundings. It frees up time for them to do other things; some of those things are work working type of things, but also things like relaxation. As a result, this evolution in the role of the driver signifies a change in what the monitoring system does changing from monitors of engagement, and readiness to take the wheel, to monitors of mood, to enhance comfort. An emotion is a biological and behavioral reaction to a feeling regarding an event that occurred in the past. In the car and elsewhere, at times drivers will likely feel discomfort with automation behavior ~ driving too fast or too slow for their tastes.

Disuse is the result of a buildup of unsatisfactory experiences, causing distrust of the driver(s) and hence the rejection of the vehicle whereby, in some cases, the decision of not using the vehicle follows. You read a lot about how hard it is to fix trust and restore acceptability: because bad moments weigh more than good, you need and much longer time and many more good experiences. However, the driver's affective state, which can be monitored in real-time, could provide an opportunity for training the automation to behave in a manner that is more consistent with the drivers' expectations and subsequently improve the drivers' experience, comfort, and trust. Combating these factors, staying in line with safety and traffic, and offering better value of travel time (Alsaid et al., 2023) automated vehicle technologies can be called upon.

Autonomous Vehicles (AVs) use a vehicle driving automation system to drive the vehicle instead of a human driver, and the primary goal of AVs is to improve road traffic safety. Compared to human drivers, AVs have better recognition, much stronger decision algorithms, and can drive much more effectively than humans; AVs can also use V2X (Vehicle-to Everything) communication technology to connect with other vehicles, dog houses, and pedestrians. By significantly reducing human errors, AV technology's progress is postulated to improve traffic conditions, reduce accident risk, and increase a safer experience on the
road for users (Cui et al., 2019)

When it comes to overcoming challenges within the adjacency of in-vehicle, Artificial Intelligence (AI) and Machine Learning (ML) steps in as the answer to a lot of the challenges in the adjacencies. AI and ML techniques, in particular have emerged as novel methodologies to address complex application domains, one of which includes securing in-vehicle networks. Potential attacks are transmitted through many channels, creating security vulnerabilities with these intelligent vehicle networks which require advanced security measures such as detection and prevention using ML-based security schemes to efficiently counter possible attacks. Combined with classic cryptographic approaches, modern authentication schemes such as biometric security, key-based authentication, and password protection are adopted to meet different security challenges involved in in-vehicle networks. For authentication purpose. The primary drawback of cryptographic techniques has been their low accuracy in the verification of real/spoofed transferred value when it comes to securing in-vehicle networks. Thus, cryptographic techniques have been widely used in low powered vehicle security systems (Rathore et al., 2022).

Since the appearance of the Autonomous Vehicle (AV) has been nothing short of spectacular, it is transforming the arena of how humans translate themselves around. Connected Vehicles (CVs) are the idea to interconnect vehicles, as well as interact with road infrastructures and the Internet, which has been now-body and typically attached to AVs. Connected and Autonomous vehicles (CAVs)

have been one of the most studied topics in both academia and the industry, that aims to usher in a driverless, safe, energy-efficient transport system. CAV public demonstrations have appeared in North America, Japan, and Europe (Minh Pham and Kaiqi Xiong 2021).

Literature Review

One of the major benefits of AVs is their potential to greatly reduce accidents and save lives. With a combination of advanced sensors, machine-learning algorithms, and sophisticated control systems, AVs can sense potential hazards and respond more quickly and accurately than a person behind the wheel. If used correctly; this could drastically decrease the number of accidents on the roads and save thousands of lives. Further, AVs can lead to improved resource use and less traffic. AVs will be smarter than the average bear: they will communicate with each other and the surrounding infrastructure to determine the most efficient routes and velocity for each vehicle to minimize travel time and improve overall traffic management. You can reduce the economic and environmental costs of congestion substantially this way. Yet, while AVs have tremendous potential, their implementation brings several challenges that must be overcome prior to making the technology a reality. A significant challenge is the lack of robust standards that govern the safety and reliability of AVs (Sadaf et al., 2023).

Akabane et al., 2020 proposed the environmental sensing layer to help in the raw data collection which can then be used to derive accurate knowledge concerning road traffic conditions. It relies on V2V and V2I communication, roadside sensors and transportation infrastructure to gather a real-time raw data traffic to form and update acknowledge base. In order to do that, vehicles occasionally communicate among themselves or with the central entity via a beacon message. A typical such a message is a raw data that is offered by the global navigation satellite system (GNSS) receiver like its current position, speed and heading, to name a few. The vehicular ad hoc networks (VANETs) have reported a high number of applications, based on vehicle to vehicle (V2V) communication, in which vehicles cooperate by sharing traffic information (sensed by sensors) to improve driving safety, traffic efficiency and convenience. In the presence of the central trusted authority and infrastructures, V2V communications are authenticated. While there hasn't been a good coverage of what happens when the infrastructures are absent. Based on this, we propose LIDAR, a lidar information-based authentication scheme for V2V communication, allowing that vehicle in a local area can authenticate themselves without a trusted authority and infrastructure. This enables the surrounding objects shared with the vehicles to be validated by making use of the sensors which the caravan of vehicles have. (A.mehmood 2016)The proposed scheme is also strong resistant to the potential security attacks like man in the middle attack (Kiho Lim; Kastuv M. Tuladhar 2019). Automated driving has emerged as one of the key technologies that can bring a revolution to the future of transport and mobility because of the constant advancements in sensor and communication technologies and the effective application of the obstacle detection techniques and algorithms. Central to perception of the surrounding environment of vehicles in an automated driving system and to the utilization and performance of multiple integrated sensors is that the safety and feasibility of automated driving vehicles can be directly determined. Sensor calibrations a building block at the core of any autonomous systems and its parts and must be accurately performed before sensor fusion along with obstacle detection processes can take place. It analyses capabilities and technical performance of sensors, widely used in autonomous vehicles, mainly covering assortment of vision cameras, LiDAR sensors and radar sensor and the wide variety of conditions in which such sensors might be operating in the practice. We talk about the three principal types of sensor calibration and review what open-source calibration packages are available to calibrate multi-sensors and how well they can be applied to a variety of commercial sensors (Yeong et al., 2021).

Two positive outcomes occur when vehicles establish network connections between them because attackers gain the ability to mount attacks against these vehicles and the entire connected transportation infrastructure along with other vehicles. Protecting connected vehicles introduces special security obstacles that are difficult to overcome. An end-to-end cloud-assisted connected vehicle security framework receives attention along with its description of

distinctive security obstacles in this paper. (Zhang, Antunes, et al., 2014)

Vehicle engines face rising cybersecurity threats because they contain progressively more sensor-based networking devices. Security solutions adopt separate protocol-specific tools at present whereas integrated standards for in-vehicle exchange protection remain absent. Preventing new cyber threats demands organizations to combine multiple defense methods thoroughly. Modern vehicles need complete security systems to defend their in-vehicle networks owing to their complicated network design. Security for ECU sensors and gateways using vehicle network communication relies on the implementation of protected standards and system arrangements. (Kornaros et al., 2020)

Routing and rebalancing a shared fleet of autonomous (i.e., self-driving) vehicles providing on-demand mobility over a capacitated transportation network that could experience congestion and therefore limit throughput. We frame the problem in a network flow setting and prove that under simply verifiable light assumptions, if the rebalancing vehicles are properly coordinated, they do not cause an increase in congestion (this conclusion is in sharp contrast to the widely held belief that congestion must ensue). From the perspective of algorithms, this theoretical result indicates that the problems of routing customers and rebalancing vehicles can be decoupled, resulting in a computationally efficient routing and rebalancing algorithm for autonomous vehicles. Numerical experiments and case studies substantiate our theoretical insights and demonstrate that the proposed algorithm outperforms the state-of-the-art point-to-point methods by preventing being overly congested on the road. Together, this paper offers a rigorous approach to the problem of congestion-aware, systemwide coordination of autonomously driving vehicles, and to the characterization of the sustainability of such robotic systems (Rossi et al., 2018).

The fastest rate of growth in the population has ruined the existing transport system in which a huge number of vehicles has been pounded. The new revolution emerging is smart cities and the only way to overcome problems like traffic jams, disorganized traffic, environmental issues, and a slow response time is through smart cities. intelligent transportation system (ITS), which is the communication, interaction, and correlation of communication between vehicles, is a part of smart cities ITS, and the mass implementation of this technology is the answer to traffic problems caused by the existing transportation system and autonomous vehicles are the central pillar of this. Specifically, centralized vehicular ad hoc networks (VANET) for external vehicular communications that are efficient and reliable lead to autonomous vehicles Malik et al. (2020).

Self-driving transport is not only an unavoidable way of life but also enables economic development for the nation. Incentives for Protection and Comfort for Autonomous Vehicles to be Extended Further Considerations for inter-vehicle communication, ideal methods for the user to interact with the autonomous vehicle, and the communication systems components for autonomous vehicles. A vehicular ad hoc network a prominent roadside communication assisted technology for this purpose has been introduced.(Ahmad, W 2025) Communication errors in transportation can be mitigated by service interruptions making information access easier. Uninterrupted communication also requires overcoming external and internal communication lags (Abbas etal., 2021).

The present literature on connected vehicle security is primarily based on reactive detection solutions and often addresses individual machine learning models, which confines their applicability to various and real-time cyber risks. Also, most explanations do not provide a thorough proportional analysis and do not reflect the dynamism of vehicular networks, such as latency and changing attack patterns. (Khan, S. A 2026), This study fills these gaps by initiating an intrusion detection framework that is built on machine learning and functions in real-time, combining continuous monitoring and evaluating various models (Decision Tree, Logistic Regression, SVM, and KNN).(Ahmad, W 2025) The study offers a more solid, precise, and scalable solution to detecting MitM and other cyberattacks in connected vehicles, based on the CARLA simulation environment and the inclusion of diverse attack scenarios.

Methodology

The proposed research is a quantitative and experimental research approach to create a strong framework in securing connected vehicles by using continuous monitoring and detection of

threats in real-time. The methodology is centered around applying machine learning to categorize and identify cyber-attacks in the automobile setting. The CARLA environment was used to create a simulation-based dataset, which was used to train and evaluate various classification models. The overall process involves data collection, preprocessing, feature engineering, model training, and performance evaluation. The purpose of the study is to compare various machine learning algorithms to find the best model to detect various kinds of cyber-attacks in connected vehicle systems.

System Model and Framework

The proposed system is based on a machine learning-driven architecture designed to monitor vehicle behavior and detect anomalies in real time. The framework consists of data acquisition, preprocessing, feature extraction, model training, and real-time attack detection. The overall architecture of the proposed system is explained in Figure 1.

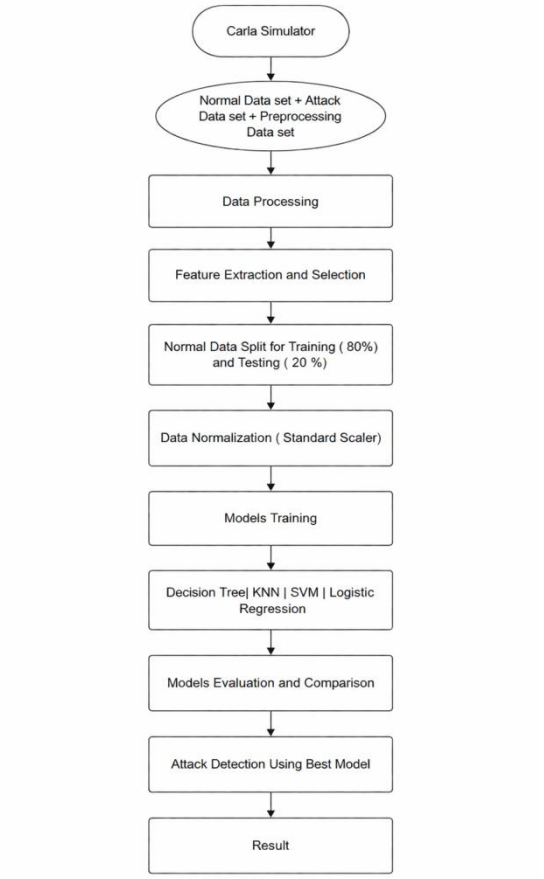

Figure 1: Architecture of the Proposed System

Dataset Description

The dataset in the present study was simulated through the CARLA simulation environment and in the form of vehicle telemetry data. The data contains throttle, brake, and steering values as the input features, and the type of attack is taken as the target variable. The dataset is classified into two categories, the normal behavior and attack behavior.

Data Preprocessing

Various preprocessing methods were used such as missing value management, invalid data elimination, dataset balancing and feature normalization with Min-Max scaling and Standard Scaler. These measures guarantee better performance and reliability of the models.

Model Selection

Four machine learning models were chosen to perform classification tasks:

Decision Tree

Decision Tree classifier is a supervised learning algorithm that models decision as a tree. The basic structure of the Decision Tree classifier is shown in Figure 2

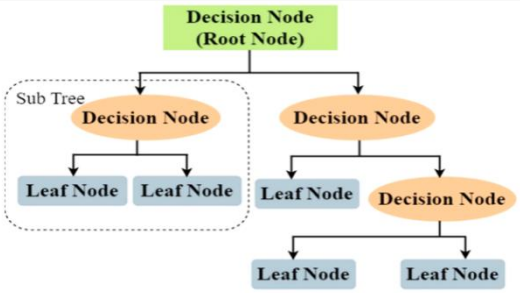

Figure 1: Basic Structure of Decision Tree

Logistic Regression

Logistic Regression is a statistical model of binary classification that estimates probabilities as a logistic regression. Figure 3 shows the structure of the Logistic Regression model.

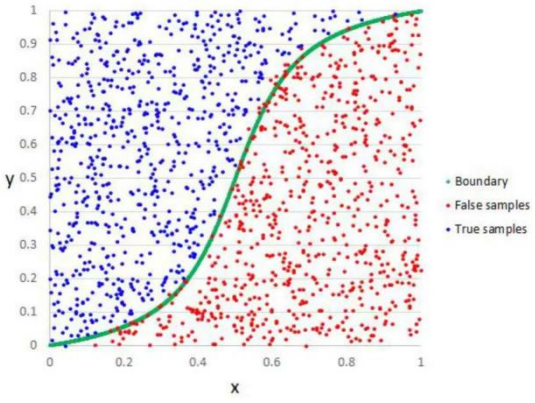

Figure 3: Logistic Regression Basic Structure

Support Vector Machine (SVM)

SVM is a supervised learning model that finds an optimal hyperplane to classify data points. The working principle of the SVM model is shown in Figure 4.

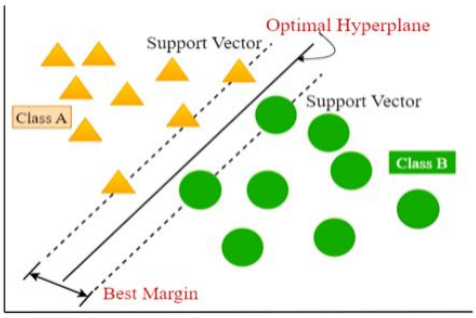

Figure 4: SVM Basic Structure

K-Nearest Neighbors (KNN) KNN is a simple classification algorithm that classifies data based on the nearest neighbors. The structure of the KNN algorithm is presented in Figure 5

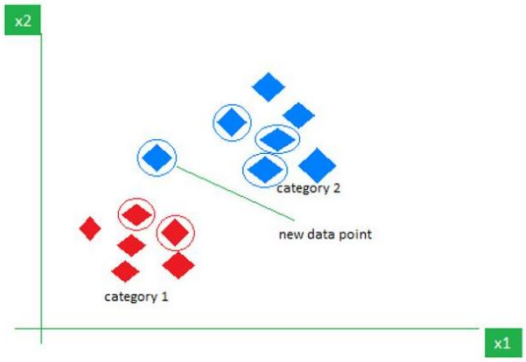

Figure 5: K-Nearest Neighbors Basic Structure

Model Training

An 80:20 ratio was used to separate the dataset into training and testing sets. The models were also trained on the basis of standardized features and tested in terms of performance

Model Evaluation

Accuracy, precision, recall, and F1-score were used to evaluate the models. A confusion matrix was also used to analyze classification performance.

Attack Scenarios

Normal Behavior (No Attack)

In normal operation, the connected vehicle behaves without any external interference. The normal operational behavior of the vehicle is shown in Figure 6

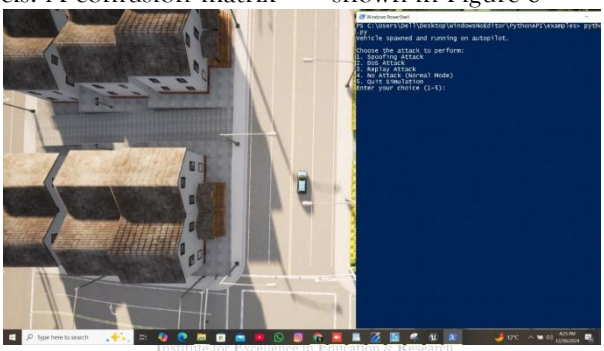

Figure 6: No Attack

Spoofing Attack

In a spoofing attack, false information is sent to the vehicle system to manipulate its behavior. The detection of spoofing attacks in the simulation environment is illustrated in Figure 7.

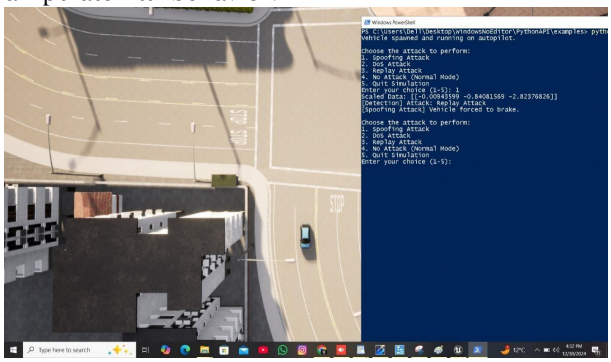

Figure 7: Connected Vehicles Detecting the Spoofing Attacks

Denial of Service (DoS) Attack

In a DoS attack, the system is overwhelmed with excessive requests, leading to instability. The detection of DoS attacks is shown in Figure 8.

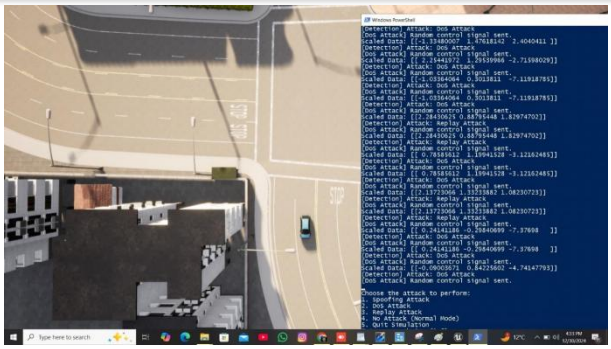

Figure 8: Connected Vehicles Detecting the DOS Attacks

Replay Attack: In a replay attack, previously recorded data is reused to manipulate the system. The replay attack detection scenario is presented in Figure 9

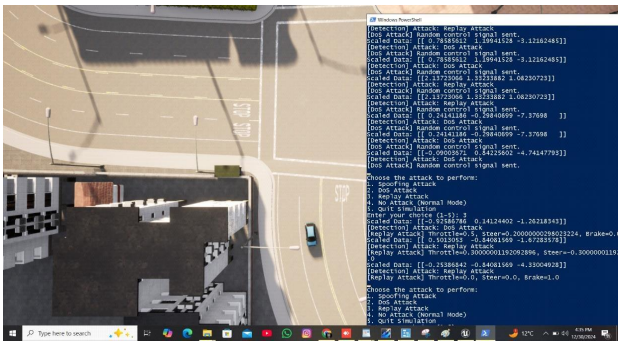

Figure 9: Connected Vehicles Detecting the Replay Attacks

Results and Discussion

The results indicate that the proposed machine learning-based framework could be useful to identify cyber-attacks in connected vehicles. Four classification models, such as Decision Tree, Logistic Regression, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN) were compared in terms of performance measures like accuracy, precision, recall, and F1-score. The highest accuracy of 97.50% was recorded in the Decision Tree classifier, which was the most successful model in the detection of normal and attack behaviors, as compared to others. The KNN model also performed better with a good accuracy of 90.00% compared to SVM and Logistic Regression, which had a 78.75% and 77.50% accuracy, respectively. These findings suggest that tree-based models have better performance on the specified dataset because of their capacity to detect nonlinear trends in vehicle telemetry data.

The classification report also specifies that the model is very good in identifying No Attack and Spoofing Attack cases with almost perfect precision and recall rates. But, on the case of Replay Attack, the performance is relatively low mainly because of the small number of samples that are available in this category. The confusion matrix analysis validates the claim that the majority of the predictions are along the diagonal, which implies that there are correct classifications and the misclassifications are minimal among the attack types. Moreover, the suggested system shows great potential in differentiating between normal and abnormal vehicle behavior within real-time simulation settings.

It is also indicated in the results that there is a significant enhancement in model performance when the preprocessing techniques, like normalization, class balancing and feature selection, are used. CARLA simulation data can be used and allow to test the proposed system under realistic conditions which will guarantee the applicability of the proposed system to the connected vehicle environment in the real world. In general, the results confirm that the suggested framework is a useful and effective tool to ensure continuous surveillance and detect threats.

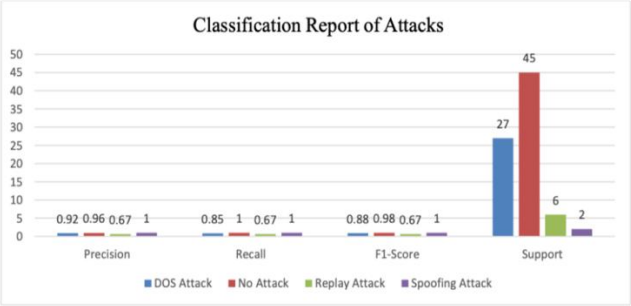

Figure 10: Classification Report of Attacks

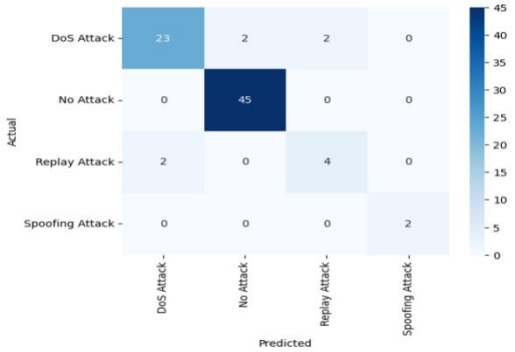

Figure 11: Confusion Matrix of attacks

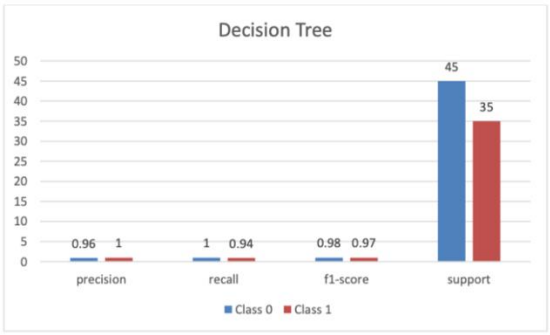

Figure 12: Classification of Decision Tree

Figure 13: Classification of Logistic Regression

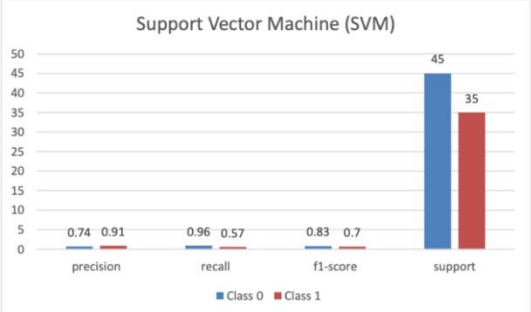

Figure 14: Classification of SVM

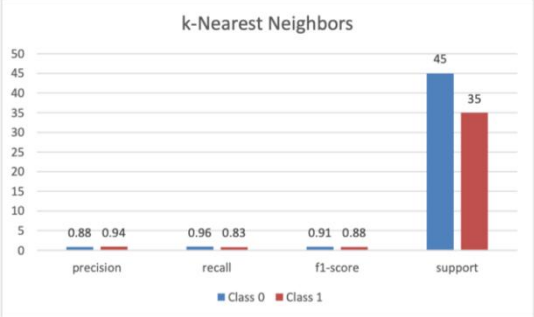

Figure 15: Classification of K-Nearest

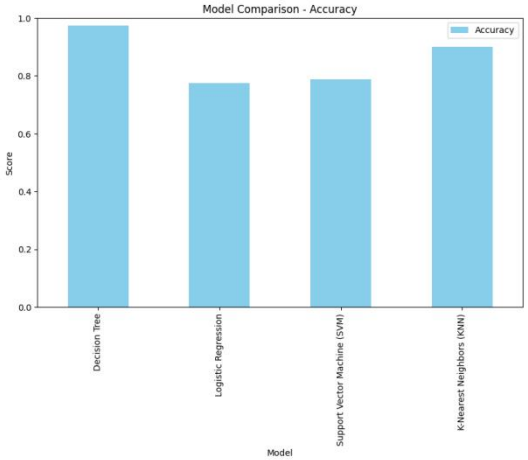

Figure 16: Trained Models Accuracy Comparison

Table 1: *Comparison of the proposed study with the existing models.*

Research Work	Method used	Accuracy (%)	Contribution
Aloqaily et al. (2019)	Hybrid IDS (DL + DT)	95.85	Cloud based intrusion detection
Rathore et al. (2022)	ML-based Security Models	~92	In-vehicle network protection
Tang et al. (2019)	Security Framework	~90	Vehicular network security
Proposed Study	DT, KNN, SVM, LR	97.50	Real-time threat detection using CARLA

As shown in the comparison in Table 1, the proposed study is competitive with current methods in connected vehicle security. Although certain studies achieve slightly higher accuracy, they tend to rely on more complex hybrid or deep learning models, incurring a greater computational cost. In comparison, the suggested framework employs light-weight machine learning models, yet the accuracy and the capability of real-time detection are high. This renders the suggested solution more feasible and effective to be used in resource-limited vehicular settings.

Discussion

The results of this paper demonstrate the need to choose the right machine learning models to detect cyber threats in connected cars. The high effectiveness of the Decision Tree classifier indicates that simpler models can be better than more complex models in the case of well-preprocessed data and the selection of features. Moreover, the paper also highlights the effects of the imbalance of datasets on the performance of the models especially in the detection of less common types of attacks like replay attacks. Also, the suggested framework has a high potential to be implemented into the real world since it is capable of conducting continuous monitoring and real-time threat detection. The data provided by simulation is controlled and gives the opportunity to test the model but in future, it will be possible to validate the model with real-world data. All in all, this paper will help advance the automotive cybersecurity arena by offering an efficient, scalable, and precise method of ensuring connected car systems are safeguarded against new cyber threats.

Conclusion

This paper offered a machine learning framework of protecting connected vehicles by continuous monitoring and real-time detection of threats. The suggested system aimed to detect and categorize cyber-attacks based on vehicle telemetry information acquired in a simulation setup. The study also sought to identify the best method to use to detect malicious activities in connected vehicle systems by implementing and testing various machine learning models, such as Decision Tree, Logistic Regression, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN). Experimental findings proved that the Decision Tree classifier was the most effective as it indicated the highest accuracy of 97.50, as well as a high level of precision and recall and F1-score. KNN model also demonstrated good results, whereas Logistic Regression and SVM showed relatively good results. The results show that machine learning algorithms, especially tree-based models, can be very useful in detecting cyber threats including spoofing, denial-of-service (DoS) and replay attacks. Moreover, the combination of preprocessing methods, such as normalization and class balancing, contributed to the overall improvement of the models. The presented framework will contribute to the sphere of automotive cybersecurity, as it offers a convenient and effective solution to detecting threats in real-time in connected vehicles. The CARLA simulation environment was used to provide realistic conditions of testing, which made the system reliable. Nevertheless, the research also revealed some weaknesses, including the relatively small size of the data and worse results in identifying replay attacks because of the imbalance of data. Further studies in the future would be to use bigger real-life data, to apply deep learning methods and to enhance the accuracy of detection of the less common types of attacks. Finally, this study shows the possibility of machine learning-based intrusion detection system in improving the security of connected vehicles. The suggested system will not only enhance the detection capabilities of the threats but also assist in the creation of safer and more reliable intelligent transportation systems, thus helping in the progress of safe autonomous and connected vehicle technologies.

References

1. Abbas, A., Krichen, M., Alroobaea, R., Malebary, S., Tariq, U., & Jalil Piran, M. (2021). An opportunistic data dissemination for autonomous vehicles communication. *Soft Computing*, 25, 11899–11912.
2. Agrawal, S., & Elger, G. (2021). Concept of infrastructure-based environment perception for IN2LAB test field for automated driving. In *2021 IEEE International Smart Cities Conference (ISC2)* (pp. 1–4). IEEE.
3. Ahangar, M. N., Ahmed, Q. Z., Khan, F. A., & Hafeez, M. (2021). A survey of autonomous vehicles: Enabling communication technologies and challenges. *Sensors*, 21, 706.
4. Akabane, A. T., Immich, R., Bittencourt, L. F., Madeira, E. R., & Villas, L. A. (2020).

Towards a distributed and infrastructure-less vehicular traffic management system. *Computer Communications*, 151, 306–319.
5. Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, 90, 101842.
6. Alsaid, A., Lee, J. D., Noejovich, S. I., & Chehade, A. (2023). The effect of vehicle automation styles on drivers' emotional state. *IEEE Transactions on Intelligent Transportation Systems*, 24, 3963–3973.
7. Bécsi, T., Aradi, S., Fehér, Á., & Gáldi, G. (2017). Autonomous vehicle function experiments with low-cost environment sensors. *Transportation Research Procedia*, 27, 333–340.
8. Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90, 101823.
9. Javed, A. R., Usman, M., Rehman, S. U., Khan, M. U., & Haghighi, M. S. (2020). Anomaly detection in automated vehicles using multistage attention-based CNN. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 4291–4300.
10. Kang, M. J., & Kang, J. W. (2016). Intrusion detection system using deep neural networks for in-vehicle security. *PLOS ONE*, 11(6), e0155781.
11. Khan, M. H., Javed, A. R., Iqbal, Z., Asim, M., & Awad, A. I. (2024). DivaCAN: Detecting in-vehicle intrusion attacks using ensemble learning. *Computers & Security*, 139, 103712.
12. Lim, K., & Tuladhar, K. M. (2019). LIDAR-based dynamic V2V authentication. In *2019 IEEE CCNC* (pp. 1–6).
13. Lu, H., Liu, Q., Tian, D., Li, Y., Kim, H., & Serikawa, S. (2019). The cognitive Internet of vehicles for autonomous driving. *IEEE Network*, 33(3), 65–73.
14. Luo, F., Jiang, Y., Zhang, Z., Ren, Y., & Hou, S. (2021). Threat analysis and risk assessment for connected vehicles. *Security and Communication Networks*, 2021, 1263820.
15. Malik, F. M., Khattak, H. A., Almogren, A., Bouachir, O., Din, I. U., & Altameem, A. (2020). Performance evaluation of data dissemination protocols. *IEEE Access*, 8, 126896–126906.
16. Maurya, D., Khaleghian, S., Sriramdas, R., Kumar, P., Kishore, R. A., Kang, M. G., & Priya, S. (2020). 3D printed graphene-based sensors for smart tires. *Nature Communications*, 11(1), 5392.
17. Muhammad, Z., Amjad, M. F., Abbas, H., Iqbal, Z., Azhar, A., Yasin, A., & Iesar, H. (2021). Evaluation of Android anti-malware tools. In *IEEE EUC* (pp. 117–124).
18. Parekh, D., Poddar, N., Rajpurkar, A., Chahal, M., Kumar, N., Joshi, G. P., & Cho, W. (2022). Review on autonomous vehicles: Progress and challenges. *Electronics*, 11, 2162.
19. Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats in autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 18(11), 2898–2915.
20. Pham, M., & Xiong, K. (2021). Security attacks and defense techniques survey. *Computers & Security*, 109, 102269.
21. Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-vehicle communication cybersecurity challenges. *Sensors*, 22, 6679.
22. Rossi, F., Zhang, R., Hindy, Y., & Pavone, M. (2018). Routing autonomous vehicles in congested networks. *Autonomous Robots*, 42, 1427–1442.
23. Sadaf, M., Iqbal, Z., Anwar, Z., Noor, U., Imran, M., & Gadekallu, T. R. (2024). Detection of DoS attacks using fuzzy logic. *Vehicular Communications*, 46, 100741.
24. Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Security and challenges. *Technologies*, 11(5), 117.
25. Shahid, J., Muhammad, Z., Iqbal, Z., Almadhor, A. S., & Javed, A. R. (2022). Trust-based attack detection in WSNs. *Computer Communications*, 191, 360–367.
26. Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. *Annual Review of Control, Robotics, and Autonomous Systems*, 1(1), 187–210.
27. Sheik, A. T., Maple, C., Epiphaniou, G., & Dianati, M. (2023). Securing cloud-assisted autonomous vehicles. *Sensors*, 24(1), 241.

28. Song, H. M., Kim, H. R., & Kim, H. K. (2016). Intrusion detection via CAN message timing. In *2016 ICOIN* (pp. 63–68). IEEE.
29. Yeong, D. J., Velasco-Hernandez, G., Barry, J., & Walsh, J. (2021). Sensor fusion in autonomous vehicles. *Sensors*, 21(6), 2140.
30. Zhang, T., Antunes, H., & Aggarwal, S. (2014). Securing connected vehicles end-to-end. *SAE Technical Paper*.
31. Tang, F., Kawamoto, Y., Kato, N., & Liu, J. (2019). Intelligent vehicular networks toward 6G. *Proceedings of the IEEE*, 108(2), 292–307.
32. Tiberti, W., Civino, R., Gavioli, N., Pugliese, M., & Santucci, F. (2023). Hybrid cryptography engine for vehicle security. *Applied Sciences*, 13(24), 13024.
33. Kornaros, G., Tomoutzoglou, O., Mbakoyiannis, D., Karadimitriou, N., Coppola, M., Montanari, E., & Gherardi, G. (2020). Secure networking in connected vehicles. *Journal of Systems Architecture*, 109, 101761.
34. Durani, A. M., Ali, M., Ahmad, R., Irfan, S., & ur Rehman, H. (2016). Identification and Verification of Vehicle using RFID Technique. *VAWKUM Transactions on Computer Sciences*, *4*(1), 36-43.
35. Ahmad, W., Mehmood, A., Zaidi, H. R., Khan, S. A., Adil, M., Zainoor, M., ... & Shaukat, Z. (2025). A Robust Deep Learning Model for Early Glaucoma Detection Using Retinal Imaging. *International Journal of Innovations in Science & Technology*, *7*(4), 2513-2526.
36. Ahmad, W., Mehmood, A., Zaidi, H. R., Khan, S. A., Adil, M., Zainoor, M., ... & Shaukat, Z. (2025). A Robust Deep Learning Model for Early Glaucoma Detection Using Retinal Imaging. *International Journal of Innovations in Science & Technology*, *7*(4), 2513-2526.
37. Khan, S. A., Mehmood, A., Ullah, A., UVES, M. G. B., Zaidi, H. R., Zainoor, M., Ahmad, W., & Adil, M. (2026). DYNAMIC SUPER FRAME ADJUSTMENT FOR DELAY MITIGATION IN IEEE 802.15. 4 CLUSTER-TREE WIRELESS SENSOR NETWORKS. *Kashf Journal of Multidisciplinary Research*, *3*(01), 111-124.