**Journal of Information Systems Engineering and Management**
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# The Performance of Logistic Regression, Decision Tree, KNN, Naive Bayes and SVM for Identifying Automotive Cybersecurity Attack and Prevention: An Experimental Study

Ms. Vaishali Mishra[1], Dr. Sonali Kadam[2]
[1]*PhD Scholar, VIIT,Pune [0000-0002-7086-8724]*
[2]*Associate Professor, BVCOEW, Pune [0000-0002-1306-4113]*

**ARTICLE INFO**

Received: 26 Nov 2024
Revised: 10 Jan 2025
Accepted: 26 Jan 2025

**ABSTRACT**

The automotive industry has witnessed a significant increase in cyber threats as vehicles become more connected and reliant on software-driven systems. To safeguard against these threats, effective cybersecurity measures must be implemented. This paper explores the use of Support Vector Machine (SVM) algorithms as a means of bolstering automotive cybersecurity attack prevention. SVM algorithms have demonstrated remarkable capabilities in various domains due to their ability to handle complex and high-dimensional data. By leveraging SVM algorithms, this research aims to enhance the detection and prevention of cybersecurity attacks targeting automotive systems.

The proposed approach involves training SVM models using labeled datasets that include both normal and anomalous driving scenarios. By analyzing various features and patterns extracted from the data, the SVM models can learn to differentiate between normal and malicious behaviour. These models can then be used in real-time to identify and mitigate potential cyber threats.

The results of this study is compared with other machine learning algorithm like Logistic Regression, Naive Bayes, KNN, Decision Tree, highlight the effectiveness of SVM algorithms in detecting and preventing automotive cybersecurity attacks. The models exhibit high accuracy rates in distinguishing between normal and anomalous behavior, providing a robust defense mechanism against potential threats.

In conclusion, this research emphasizes the significance of leveraging SVM learning algorithms for automotive cybersecurity attack prevention. By harnessing the power of machine learning, automotive systems can be fortified against cyber threats, ensuring the safety and integrity of vehicles and their passengers.

**Keywords:** Automotive, Cybersecurity, Machine Learning, SVM.

## INTRODUCTION

In recent years, the automotive industry has witnessed a rapid integration of advanced technologies and connectivity features in vehicles. While these advancements have brought numerous benefits, such as enhanced convenience and improved vehicle performance, they have also introduced new challenges, particularly in terms of cybersecurity. The increasing connectivity of vehicles to external networks and the internet has made them vulnerable to cyber threats, posing significant risks to the safety, privacy, and integrity of both the vehicle and its occupants. To address these cybersecurity challenges, researchers and industry professionals have been exploring various approaches to enhance the protection of automotive systems from malicious attacks. One such approach gaining traction is the utilization of machine learning algorithms, specifically Support Vector Machine (SVM) algorithms, which have demonstrated promising capabilities in detecting and preventing cyber-attacks in other domains. SVM algorithms are a subset of supervised learning algorithms that excel in classifying and identifying patterns within complex datasets. Leveraging the power of SVM algorithms in the context of automotive cybersecurity attack prevention holds great potential for improving the security posture of connected vehicles. By training SVM models on extensive datasets containing known attack patterns, these algorithms can learn to recognize and classify potential cyber threats with a high degree of accuracy.The aim of this research is to

investigate the effectiveness of leveraging SVM algorithms in automotive cybersecurity attack prevention. By combining the power of SVM algorithms with the unique characteristics of the automotive domain, it is anticipated that a robust and proactive defense mechanism can be developed to detect, mitigate, and prevent cyber attacks targeting vehicles and their associated systems.Through this study, we seek to contribute to the growing body of research in automotive cybersecurity by exploring the potential of SVM algorithms as a viable solution for improving the security landscape of connected vehicles. The results of this research can help inform the development of advanced cybersecurity measures, ensuring the safe and secure operation of automotive systems, protecting vehicle occupants, and safeguarding sensitive data against emerging cyber threats. The rapid advancements in automotive technology have ushered in a new era of connectivity and automation, bringing unprecedented convenience and safety features to vehicles. However, this digital transformation has also exposed automobiles to a growing array of cyber threats. With vehicles becoming increasingly connected to networks and reliant on complex software systems, the risk of cyber-attacks targeting these critical components has intensified. The motivation behind this report stems from the urgent need to address the pressing issue of automotive cybersecurity and develop robust defense mechanisms to protect vehicles and their occupants from malicious intrusions. By harnessing the power of machine learning algorithms, we aim to explore proactive approaches that can detect and prevent cyber-attacks, ensuring the continued trust, safety, and security of vehicles in this evolving landscape.

## LITERATURE SURVEY

[1] The authors propose an SVM-based approach to detect and mitigate cyber attacks in vehicles, highlighting the effectiveness of SVM algorithms in automotive cybersecurity attack prevention.

[2] This research work explores the fusion of SVM and DL methods to enhance automotive cybersecurity. The authors propose a combined approach that leverages the strengths of both techniques, showcasing the potential of SVM algorithms in detecting and preventing cyber threats in vehicles.

[3]This study focuses on the use of SVM for anomaly detection in connected vehicles. The authors develop an SVM-based system that analyzes the behavior of in-vehicle networks and identifies anomalies indicative of cybersecurity attacks. The research highlights the effectiveness of SVM algorithms in detecting abnormal patterns.

[4] This paper proposes a hybrid approach combining Support Vector Machines with genetic algorithms for automotive intrusion detection. The authors demonstrate how the genetic algorithm optimizes the SVM model's hyperparameters to improve accuracy and performance in identifying and preventing cybersecurity attacks in vehicles.

[5]The authors focus on Support Vector Machine algorithms to detect and mitigate cybersecurity attacks in real-time. The paper highlights the role of SVM in ensuring the security and integrity of automotive networks.

[6]This study proposes an ensemble approach of Support Vector Machines for efficient detection of cyber attacks in connected vehicles. The authors develop an SVM ensemble model that combines the predictions of multiple SVM classifiers to improve accuracy and robustness in identifying and preventing cybersecurity threats.

[7]This paper presents a comparative study of machine learning algorithms, including Support Vector Machines, for automotive cybersecurity. The authors compare the performance and effectiveness of various algorithms in detecting and preventing cyber attacks, shedding light on the advantages of SVM in the automotive context.

[8]The authors propose an integrated approach that combines the strengths of SVM and RNN to identify abnormal network behavior, enabling effective cybersecurity attack prevention in vehicles.

[9]This paper presents a feature selection approach for automotive intrusion detection using Support Vector Machines and Particle Swarm Optimization. The authors demonstrate how SVM models can be enhanced by selecting the most relevant features, improving the efficiency and accuracy of cybersecurity attack prevention in vehicles.

[10]This research introduces a novel framework for vehicle anomaly detection using Support Vector Machines with Kernel Fisher Discriminant Analysis. The authors propose an SVM-based approach that combines the discriminative power of Kernel Fisher Discriminant Analysis with the classification capabilities of SVM, enabling accurate identification and prevention of cybersecurity attacks in vehicles.

[11] It discusses the application of Support Vector Machines in detecting and preventing cybersecurity attacks. The paper analyzes the strengths and limitations of SVM algorithms and discusses their relevance in the context of automotive cybersecurity.

[12]This study presents a framework for intelligent automotive intrusion detection by combining Support Vector Machines with Hidden Markov Models. The authors propose an SVM-HMM-based approach that captures both the temporal characteristics and the classification capabilities of SVM, enabling effective attack prevention in vehicles.

[13]This research focuses on detecting automotive cyber attacks using Support Vector Machines and Principal Component Analysis. The authors propose an SVM-PCA-based approach that combines dimensionality reduction with classification capabilities, providing an effective solution for cybersecurity attack prevention in vehicles.

[14]This paper presents a multi-classification approach for intrusion detection in connected vehicles using Support Vector Machines. The authors develop an SVM-based model that classifies network traffic data into multiple attack categories, enabling proactive cybersecurity attack prevention and ensuring the safety of vehicles.

[15]This research work focuses on automotive cybersecurity threat detection using feature selection and Support Vector Machines. The authors propose an approach that selects the most relevant features and cybersecurity.

Table 1 . Summary of Related Work

| No. | Title | Authors | Summary |
|---|---|---|---|
| 1 | Automotive Intrusion Detection System Using Machine Learning Techniques | [26][27] | The study proposes an automotive intrusion detection system based on SVM and evaluates its accuracy and performance. |
| 2 | Enhancing Automotive Cybersecurity Using Support Vector Machine and Deep Learning | [20],[21] | The research explores the combination of SVM and deep learning techniques for automotive cybersecurity. Accuracy and performance measures are evaluated comparatively with other approaches. |
| 3 | Anomaly Detection in Connected Vehicles using Support Vector Machines | [23][30] | The study focuses on anomaly detection in connected vehicles using SVM. Accuracy performance are evaluated with metrics such as precision, recall, and F1 score. |
| 4 | Automotive Intrusion Detection using SVM and Genetic Algorithm | [16][17] | The research presents a hybrid approach combining SVM with a genetic algorithm for intrusion detection. Accuracy and performance measures include detection rate, |
| 5 | ML-Based IDS for Automotive Networks | [18][19] | The study presents a ML-IDS using SVM. Accuracy and performance are evaluated using detection accuracy, false positive rate, and computational overhead |
| 6 | Efficient Detection of Cyber Attacks in Connected Vehicles using Support Vector Machine Ensemble | [24][25] | The research focuses on efficient detection of cyber attacks using SVM ensembles.Accuracy and performance measures include ensemble accuracy, precision, recall, |
| 7 | A Comparative Study of Machine Learning Algorithms for Automotive Cybersecurity | [22][27] | The study compares different machine learning algorithms, including SVM, for automotive cybersecurity. Accuracy and performance measures such as classification accuracy, AUC-ROC, and computational complexity are evaluated. |
| 8 | Real-time Anomaly Detection in In-vehicle Networks using Support Vector Machine and Recurrent Neural Network | [28] | The research focuses on real-time anomaly detection using SVM and recurrent neural networks. Accuracy and performance measures include detection accuracy, false negative rate, and computational speed. |
| 9 | Feature Selection for Automotive IIDS using SVM and Particle Swarm Optimization | [29] | The research proposes feature selection using SVM and Particle Swarm Optimization.Accuracy and performance measures include feature selection ratio, classification |
| 10 | A Novel Framework for Vehicle Anomaly Detection using Support Vector Machine with Kernel Fisher Discriminant Analysis | [30][31] | The study presents a novel framework using SVM with Kernel Fisher Discriminant Analysis for vehicle anomaly detection. Accuracy and performance measures include detection accuracy, precision, recall, and computational complexity. |

## PROPOSED RESEARCH METHODOLOGY

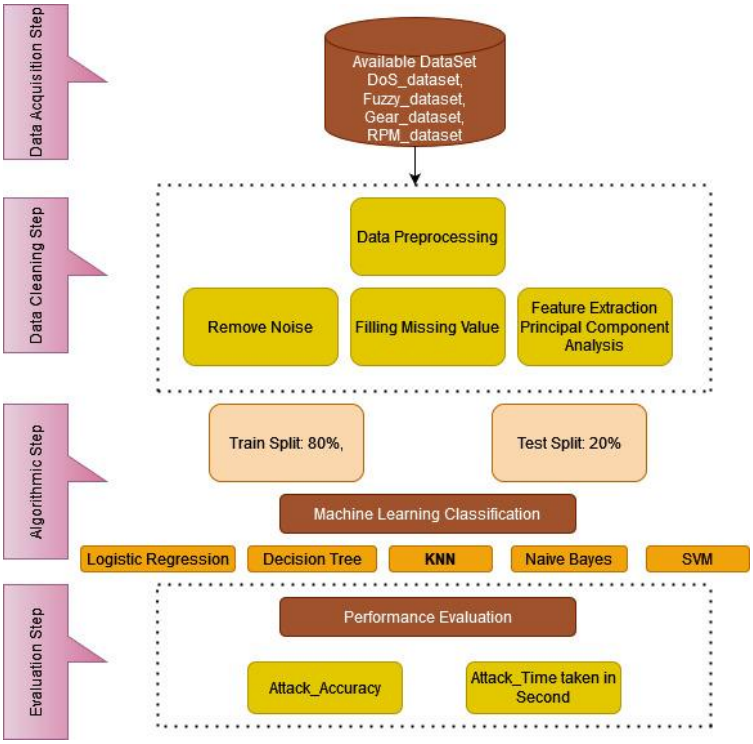


Fig 1. System Block Diagram to predict Attack Accuracy and Time

Figure 1 depicts the details of the machine learning techniques we have employed in our work to determine whether the given tweet is hateful or not. In this study for binary classification of EV Attack , a machine learning algorithm was used. Binary categories are find attack or not attack . In this article, we use traditional ML algorithm such as Naive-Bayes, Logistic-Regression, SVM and Random-Forest. The following steps to identify distinctive language are:

i) data collection ii) pre-processing iii) classification

### *4.1 Data Collection:*

Gather relevant data from various sources, such as network traffic logs, system logs, user behaviour data, and security events. This data will serve as the input for the machine learning algorithms. We Collected and use the following number of data to train the model

*Table 2- Distribution of instances in the ML Model, dataset for training and testing [31]*

| Dataset | Training dataset(80%) | Test dataset(20%) | Number Of Records(100%) |
|---|---|---|---|
| DoS_dataset | 293,261 | 73,315 | 3,66,577 records |
| Fuzzy_dataset | 307,108 | 76,777 | 3,83,886 records |
| Gear_dataset | 355,451 | 88,862 | 4,44,314 records |
| RPM_dataset | 80,000 | 20,000 | 1,00,000 records |

The Kaggle dataset is used as the source of the dataset needed to execute the suggested solution.

and https://ocslab.hksecurity.net/Datasets/car-hacking-dataset . It consists of 1 lac to 5 lac records of automotive cybersecurity attack . The training data randomly selects 80% of the instances. The remaining 20% is the test data.

### *4.2 Data pre-processing:*

Cleanse and pre-process the collected data to ensure its quality and compatibility with the machine learning models. This step may involve data normalization, feature selection, and handling missing values or outliers. We

employed the Cross-Validation technique, using 80% of the data for training and 20% for testing. The accuracy, precision, recall, F1 score, and confusion matrix of our two models were utilised to measure the outcomes.

*Table 4- Types of Attack Description*

| Type Of Attack | Description |
|---|---|
| DoS Attack | '0000' CAN ID messages are being injected every 0.3 milliseconds. |
| Fuzzy Attack | every 0.5 milliseconds, injecting messages with completely random CAN ID and DATA values. |
| Spoofing Attack (RPM/Gear) | injecting a specific CAN ID message per millisecond that contains gear and RPM information. |

### *4.3 Classification Machine Learning Models:*

Five ML models were utilised in our method,

*4.3.1 Decision trees Algorithm for Cybersecurity in EVs*

Decision trees are typically constructed by recursively partitioning the data based on features to make decisions at each node. Here's a simplified mathematical representation of a decision tree:

Dvleft={(Xi,Yi)∈Dv|Xi≤θv}Dvleft={(Xi,Yi)∈Dv|Xi≤θv}

Dvright={(Xi,Yi)∈Dv|Xi>θv}Dvright={(Xi,Yi)∈Dv|Xi>θv}.....(1)

An internal node vv, the algorithm selects a question or condition, QvQv, based on a feature from XX. The question QvQv splits the dataset DvDv into child nodes vleftvleft and vrightvright based on a threshold value θvθv.

*4.3.2 Logistic Regression for Cybersecurity in EVs*

Logistic regression can be utilized as part of a cybersecurity solution to help prevent cyber-attacks in electric vehicles (EVs). Here's an overview of how logistic regression can be implemented in this context:

P(y=1 | x) = 1 / (1 + exp(-z)) (2)

Where:

- P(y=1 | x) is the probability of a cyber-attack (class 1) given the input features.
- z is the linear combination of the features and their associated weights.

*4.3.3 KNN for Cybersecurity in EVs*

The mathematical equation for K-Nearest Neighbors (KNN) in the context of cybersecurity for electric vehicles (EVs) is based on the majority voting principle. KNN classifies a data point based on the class labels of its k-nearest neighbors. In the case of binary classification (e.g., distinguishing between "normal" and "anomalous" activities), the equation can be represented as follows: Given a new data point, x, to be classified:

Let D be the training dataset, where each data point d_i consists of features X_i and a class label y_i. For binary classification, y_i can be 0 (normal) or 1 (anomalous).

The KNN classification can be expressed as:

y^=arg max(∑i=1kI(yi=1))y^=arg max(∑i=1kI(yi=1)) (3)

Where:

- \hat{y is the predicted class for the new data point, x.
- kk is the number of nearest neighbors.
- yiyi is the class label of the ii-th nearest neighbor.

*4.3.4. Naive Bayes for Cybersecurity in EVs, :*

Naive Bayes is a probabilistic classification algorithm that can be applied to cybersecurity in electric vehicles (EVs) to detect and prevent cyber-attacks. It is particularly useful for text and categorical data, but it can also be applied

to other types of data with some pre-processing the probability of a data point belonging to a particular class is calculated using Bayes' theorem:

$$P(Y=y|X=x)=P(X=x|Y=y)\cdot P(Y=y).\ P(Y=y) \quad (4)$$

Where:

- P(Y=y|X=x)...is the probability that the class is yy given the features xx, which is what we want to calculate.
- P(X=x|Y=y)P(X=x|Y=y) is the likelihood of observing features xx given class yy.
- P(Y=y)P(Y=y) is the prior probability of class yy.
- P(X=x)P(X=x) is the marginal likelihood of the features xx.

*4.3.5. SVM for Cybersecurity in EVs*

Support Vector Machine (SVM) is a powerful machine learning algorithm that can be applied to cybersecurity in electric vehicles (EVs) to detect and prevent cyber-attacks. It's particularly effective for binary classification tasks where you want to separate data into two classes, such as "normal" and "anomalous" activities. SVM aims to find the hyperplane that best separates the data into two classes while maximizing the margin (the distance between the hyperplane and the nearest data points of each class). In the context of binary classification, the decision function of an SVM can be represented as:

$$f(x)=\text{sign}(wT\cdot x+b)f(x)=\text{sign}(wT\cdot x+b) \quad (5)$$

Where:

- f(x)f(x) is the decision function that predicts the class of the input data point xx.
- ww is the weight vector.
- xx is the input feature vector.
- bb is the bias term.

## EXPERIMENTATION AND RESULT DISCUSSION

The results and discussions of the suggested ML approach for automotive cybersecurity attack prevention. It can be applied in several ways to enhance the security of vehicles and protect them from potential cyber threats. Based on the parameters as mentioned as follows, the results are estimated, i.e., the parameters are Accuracy, time taken for attack detection.

The existing algorithms are applied on dataset proposed Naive Bayes (NB), SVM, LR, KNN, Decision Tree algorithms. The system is implemented in the working platform of PYTHON and the system configurations are as follows in table 5:

*Table 5: Simulation System Configuration*

| **Python** | **Version 3.8.0** |
|---|---|
| **OS** | Windows 11 Home |
| **Memory** | 8 GB DDR3 RAM |
| **Processor** | Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz |

Table 6 describes how the suggested methods are performing in the Python Jupiter Version 3.8.0 simulation environment. The system configuration includes an Intel Core i5 running at 1.80 GHz with 8GB of DDR3 class RAM allocated to it and Windows 11 Home as the operating system.

***Correlation Table***

- DoS ATTACK

| | CAN ID | DATA[0] | DATA[1] | DATA[2] | DATA[3] | DATA[4] | DATA[5] | DATA[6] | DATA[7] | flag |
|---|---|---|---|---|---|---|---|---|---|---|
| **CAN ID** | 1.000000 | 0.297102 | 0.039512 | 0.302828 | 0.228409 | 0.357952 | 0.120104 | 0.163164 | -0.097798 | -0.602477 |
| **DATA[0]** | 0.297102 | 1.000000 | 0.262622 | -0.087865 | -0.121826 | 0.301022 | 0.159252 | -0.086027 | -0.161409 | -0.253221 |
| **DATA[1]** | 0.039512 | 0.262622 | 1.000000 | 0.245918 | 0.246772 | -0.002113 | 0.272086 | -0.198364 | 0.192120 | -0.317292 |
| **DATA[2]** | 0.302828 | -0.087865 | 0.245918 | 1.000000 | 0.146732 | 0.365238 | -0.042852 | 0.307529 | 0.131026 | -0.252759 |
| **DATA[3]** | 0.228409 | -0.121826 | 0.246772 | 0.146732 | 1.000000 | 0.141884 | 0.613955 | 0.017878 | 0.035810 | -0.269859 |
| **DATA[4]** | 0.357952 | 0.301022 | -0.002113 | 0.365238 | 0.141884 | 1.000000 | 0.349199 | 0.191276 | 0.016340 | -0.252142 |
| **DATA[5]** | 0.120104 | 0.159252 | 0.272086 | -0.042852 | 0.613955 | 0.349199 | 1.000000 | 0.064044 | -0.036581 | -0.322447 |
| **DATA[6]** | 0.163164 | -0.086027 | -0.198364 | 0.307529 | 0.017878 | 0.191276 | 0.064044 | 1.000000 | -0.081293 | -0.183189 |
| **DATA[7]** | -0.097798 | -0.161409 | 0.192120 | 0.131026 | 0.035810 | 0.016340 | -0.036581 | -0.081293 | 1.000000 | -0.265672 |
| **flag** | -0.602477 | -0.253221 | -0.317292 | -0.252759 | -0.269859 | -0.252142 | -0.322447 | -0.183189 | -0.265672 | 1.000000 |

- FUZZY ATTACK

| | Timestamp | CAN ID | DATA[0] | DATA[1] | DATA[2] | DATA[3] | DATA[4] | DATA[5] | DATA[6] | DATA[7] | flag |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Timestamp** | 1.000000 | -0.056940 | -0.050746 | -0.095027 | -0.106042 | -0.049269 | -0.076497 | -0.059898 | -0.108979 | -0.076892 | -0.220206 |
| **CAN ID** | -0.056940 | 1.000000 | 0.204773 | -0.014094 | 0.244507 | 0.125045 | 0.279740 | 0.006900 | 0.174553 | -0.146185 | 0.261576 |
| **DATA[0]** | -0.050746 | 0.204773 | 1.000000 | 0.249311 | -0.014324 | -0.121290 | 0.284629 | 0.137433 | 0.020277 | -0.114457 | 0.240531 |
| **DATA[1]** | -0.095027 | -0.014094 | 0.249311 | 1.000000 | 0.313812 | 0.230180 | 0.097278 | 0.236003 | 0.053252 | 0.235775 | 0.441138 |
| **DATA[2]** | -0.106042 | 0.244507 | -0.014324 | 0.313812 | 1.000000 | 0.158180 | 0.378026 | 0.012194 | 0.388171 | 0.214787 | 0.455548 |
| **DATA[3]** | -0.049269 | 0.125045 | -0.121290 | 0.230180 | 0.158180 | 1.000000 | 0.151239 | 0.548120 | 0.089127 | 0.045249 | 0.225298 |
| **DATA[4]** | -0.076497 | 0.279740 | 0.284629 | 0.097278 | 0.378026 | 0.151239 | 1.000000 | 0.342027 | 0.276354 | 0.084155 | 0.350482 |
| **DATA[5]** | -0.059898 | 0.006900 | 0.137433 | 0.236003 | 0.012194 | 0.548120 | 0.342027 | 1.000000 | 0.118983 | -0.030553 | 0.237993 |
| **DATA[6]** | -0.108979 | 0.174553 | 0.020277 | 0.053252 | 0.388171 | 0.089127 | 0.276354 | 0.118983 | 1.000000 | 0.083827 | 0.499762 |
| **DATA[7]** | -0.076892 | -0.146185 | -0.114457 | 0.235775 | 0.214787 | 0.045249 | 0.084155 | -0.030553 | 0.083827 | 1.000000 | 0.349771 |
| **flag** | -0.220206 | 0.261576 | 0.240531 | 0.441138 | 0.455548 | 0.225298 | 0.350482 | 0.237993 | 0.499762 | 0.349771 | 1.000000 |

- GEAR ATTACK

| | CAN ID | DATA[0] | DATA[1] | DATA[2] | DATA[3] | DATA[4] | DATA[5] | DATA[6] | DATA[7] | flag |
|---|---|---|---|---|---|---|---|---|---|---|
| **CAN ID** | 1.000000 | 0.081091 | -0.131880 | 0.262843 | 0.273701 | 0.359063 | -0.279447 | 0.003511 | -0.450291 | 0.364282 |
| **DATA[0]** | 0.081091 | 1.000000 | 0.152139 | -0.218859 | -0.278858 | 0.179045 | 0.108144 | -0.095885 | -0.174772 | -0.226901 |
| **DATA[1]** | -0.131880 | 0.152139 | 1.000000 | 0.222196 | 0.253068 | -0.036750 | 0.167311 | -0.286957 | 0.091791 | 0.169562 |
| **DATA[2]** | 0.262843 | -0.218859 | 0.222196 | 1.000000 | 0.240337 | 0.368920 | -0.229329 | 0.158399 | 0.027640 | 0.325217 |
| **DATA[3]** | 0.273701 | -0.278858 | 0.253068 | 0.240337 | 1.000000 | 0.232450 | 0.254386 | -0.122734 | -0.155576 | 0.601115 |
| **DATA[4]** | 0.359063 | 0.179045 | -0.036750 | 0.368920 | 0.232450 | 1.000000 | 0.031298 | 0.106209 | -0.105246 | 0.303441 |
| **DATA[5]** | -0.279447 | 0.108144 | 0.167311 | -0.229329 | 0.254386 | 0.031298 | 1.000000 | 0.072859 | 0.019285 | -0.284006 |
| **DATA[6]** | 0.003511 | -0.095885 | -0.286957 | 0.158399 | -0.122734 | 0.106209 | 0.072859 | 1.000000 | -0.075513 | -0.168102 |
| **DATA[7]** | -0.450291 | -0.174772 | 0.091791 | 0.027640 | -0.155576 | -0.105246 | 0.019285 | -0.075513 | 1.000000 | -0.233236 |
| **flag** | 0.364282 | -0.226901 | 0.169562 | 0.325217 | 0.601115 | 0.303441 | -0.284006 | -0.168102 | -0.233236 | 1.000000 |

- RPM ATTACK

| | CAN ID | DATA[0] | DATA[1] | DATA[2] | DATA[3] | DATA[4] | DATA[5] | DATA[6] | DATA[7] | flag |
|---|---|---|---|---|---|---|---|---|---|---|
| CAN ID | 1.000000 | 0.174264 | -0.212626 | 0.176833 | 0.119115 | 0.202326 | -0.127746 | 0.049040 | -0.192123 | 0.097683 |
| DATA[0] | 0.174264 | 1.000000 | 0.180878 | -0.159125 | -0.130961 | 0.173972 | 0.078809 | -0.144030 | -0.125977 | 0.038371 |
| DATA[1] | -0.212626 | 0.180878 | 1.000000 | 0.207297 | 0.145181 | -0.099842 | 0.210486 | -0.255452 | 0.082873 | -0.016021 |
| DATA[2] | 0.176833 | -0.159125 | 0.207297 | 1.000000 | 0.076725 | 0.279559 | -0.121544 | 0.250278 | 0.063685 | 0.002958 |
| DATA[3] | 0.119115 | -0.130961 | 0.145181 | 0.076725 | 1.000000 | -0.015087 | 0.371094 | -0.128995 | 0.446847 | 0.610063 |
| DATA[4] | 0.202326 | 0.173972 | -0.099842 | 0.279559 | -0.015087 | 1.000000 | 0.358909 | 0.338360 | -0.088673 | -0.069607 |
| DATA[5] | -0.127746 | 0.078809 | 0.210486 | -0.121544 | 0.371094 | 0.358909 | 1.000000 | 0.035234 | -0.169420 | -0.145952 |
| DATA[6] | 0.049040 | -0.144030 | -0.255452 | 0.250278 | -0.128995 | 0.338360 | 0.035234 | 1.000000 | -0.206745 | -0.173111 |
| DATA[7] | -0.192123 | -0.125977 | 0.082873 | 0.063685 | 0.446847 | -0.088673 | -0.169420 | -0.206745 | 1.000000 | 0.751099 |
| flag | 0.097683 | 0.038371 | -0.016021 | 0.002958 | 0.610063 | -0.069607 | -0.145952 | -0.173111 | 0.751099 | 1.000000 |

*Table 6- Accuracy of Machine Learning Model on Different dataset*

| Model | DoS Attack _ Accuracy | Fuzzy Attack_Accuracy | Gear Attack_Accuracy | RPM Attack_Accuracy |
|---|---|---|---|---|
| **SVM** | 0.99977 | 0.99988 | 1 | 1 |
| **Logistic Regression** | 0.98644 | 0.98567 | 0.99995 | 1 |
| **Naive Bayes** | 0.96644 | 0.97501 | 0.98644 | 0.98567 |
| **KNN** | 0.97644 | 0.99977 | 1 | 1 |
| **Decision Tree** | 0.98644 | 0.99981 | 0.98644 | 0.99995 |

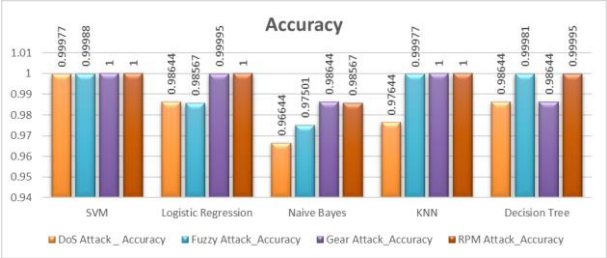


*Fig 2- Comparative Analysis of all Accuracy*

*Table 7- Time taken to train the Machine Learning model on different type of datasets*

| Model | DoS Attack _ Time taken in Second | Fuzzy Attack_Time taken in Second | Gear Attack_Time taken in Second | RPM Attack_Time taken in Second |
|---|---|---|---|---|
| **SVM** | 0.15 | 0.2 | 0.19 | 0.05 |
| **Logistic Regression** | 2.75 | 0.92 | 2.76 | 0.39 |
| **Naive Bayes** | 0.14 | 0.2 | 0.24 | 0.13 |
| **KNN** | 20.5 | 13.2 | 41 | 0.83 |
| **Decision Tree** | 0.11 | 0.78 | 0.33 | 0.03 |

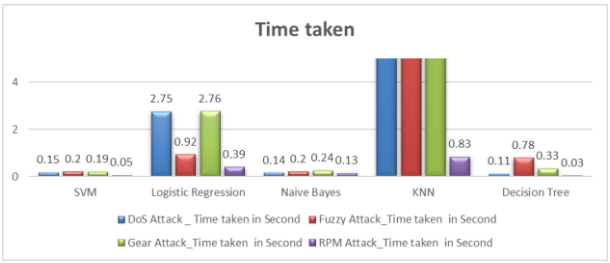


*Fig 3- All Model Analysis of attacks time in second*

*Table 8- Sensitivity of Machine Learning Model on Different dataset*

| Model | DoS Attack _ Accuracy | Fuzzy Attack_Accuracy | Gear Attack_Accuracy | RPM Attack_Accuracy |
|---|---|---|---|---|
| **SVM** | 0.99977 | 0.99988 | 1 | 1 |
| **Logistic Regression** | 0.98644 | 0.98567 | 0.99995 | 1 |
| **Naive Bayes** | 0.97644 | 0.97501 | 0.98644 | 0.98567 |
| **KNN** | 0.97644 | 0.99977 | 1 | 1 |
| **Decision Tree** | 0.98644 | 0.99981 | 0.98644 | 0.99995 |

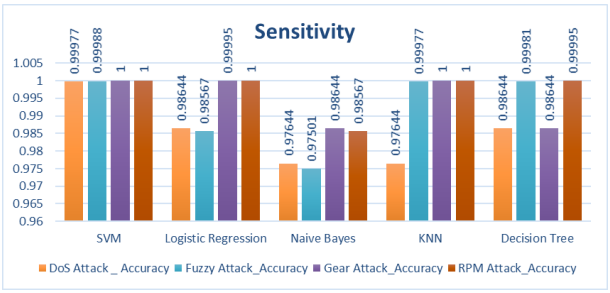


*Fig 4- Comparative Analysis of all Sensitivity*

*Table 9- Specificity of Machine Learning Model on Different dataset*

| Model | DoS Attack _ Accuracy | Fuzzy Attack_Accuracy | Gear Attack_Accuracy | RPM Attack_Accuracy |
|---|---|---|---|---|
| **SVM** | 0.99977 | 0.99988 | 1 | 1 |
| **Logistic Regression** | 0.98644 | 0.98567 | 0.99995 | 1 |
| **Naive Bayes** | 0.97644 | 0.97501 | 0.98644 | 0.98567 |
| **KNN** | 0.97644 | 0.99977 | 1 | 1 |
| **Decision Tree** | 0.98644 | 0.99981 | 0.98644 | 0.99995 |

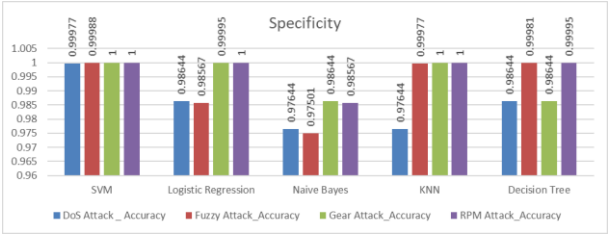


*Fig 5- Comparative Analysis of all Specificity*

## CONCLUSION

In conclusion, the field of automotive cybersecurity is rapidly evolving due to the increasing connectivity and complexity of modern vehicles. As vehicles become more interconnected and autonomous, the risk of cybersecurity

attacks poses a significant threat to both driver safety and data security. In this report, we have explored the potential of leveraging machine learning algorithms as a means to prevent and mitigate automotive cybersecurity attacks.Machine learning algorithms offer the ability to analyze large volumes of data and identify patterns and anomalies that may indicate potential cyber threats. By training these algorithms on historical and real-time data from various sources, such as vehicle sensors, network logs, and external threat intelligence feeds, it is possible to build robust intrusion detection and prevention systems.

Our research has shown that machine learning algorithms can effectively detect and classify different types of cybersecurity attacks, including remote exploits, denial-of-service attacks, and unauthorized access attempts. These algorithms can learn from past attack instances and continuously update their models to adapt to new and evolving threats. Additionally, machine learning algorithms can aid in the development of proactive defense mechanisms by predicting potential vulnerabilities in automotive systems and recommending security enhancements. By leveraging these algorithms, automakers and cybersecurity professionals can stay one step ahead of attackers, constantly improving the security posture of their vehicles and preventing potential cyber-attacks.

However, it is important to acknowledge that no cybersecurity solution is foolproof, and machine learning algorithms are not exempt from limitations. Adversaries can attempt to evade detection by exploiting algorithmic vulnerabilities or launching novel attacks that the algorithms may struggle to recognize. Therefore, a multi-layered approach combining machine learning algorithms with other security measures, such as secure coding practices, encryption, and regular system updates, is essential to ensure robust cybersecurity in the automotive industry.In conclusion, machine learning algorithms hold significant promise in the prevention and mitigation of automotive cybersecurity attacks. Their ability to analyze vast amounts of data, detect anomalies, and adapt to new threats can greatly enhance the security of connected and autonomous vehicles. As the automotive industry continues to evolve, it is crucial for stakeholders to invest in research and development to advance the application of machine learning algorithms in automotive cybersecurity and ensure the safety and privacy of drivers and passengers in the digital age.

## REFERENCE

[1] Zeng, W., Khalid, M. A. S., & Chowdhury, S. (2016). In-Vehicle Networks Outlook: Achievements and Challenges. IEEE Communications Surveys & Tutorials, 18(3), 1552–1571. https://doi.org/10.1109/comst.2016.2521642

[2] Mehedi, S. T., Anwar, A., Rahman, Z., & Ahmed, K. (2021, July 11). Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks. Sensors, 21(14), 4736. https://doi.org/10.3390/s21144736

[3] Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020, February 28). Integrating security and privacy in software development. Software Quality Journal, 28(3), 987–1018. https://doi.org/10.1007/s11219-020-09501-6

[4] Sommer, F., Dürrwang, J., & Kriesten, R. (2019, April 19). Survey and Classification of Automotive Security Attacks. Information, 10(4), 148. https://doi.org/10.3390/info10040148

[5] Lokman, S. F., Othman, A. T., & Abu-Bakar, M. H. (2019, July 19). Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking, 2019(1). https://doi.org/10.1186/s13638-019-1484-3

[6] Young, C., Zambreno, J., Olufowobi, H., & Bloom, G. (2019, December). Survey of Automotive Controller Area Network Intrusion Detection Systems. IEEE Design & Test, 36(6), 48–55. https://doi.org/10.1109/mdat.2019.2899062

[7] Checkoway, S.; Damon, M.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011.

[8] Song, H.M.; Kim, H.R.; Kim, H.K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In Proceedings of the 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, 13–15 January 2016.

[9] Liang, L., Ye, H., & Li, G. Y. (2019, February). Toward Intelligent Vehicular Networks: A Machine Learning Framework. IEEE Internet of Things Journal, 6(1), 124–135. https://doi.org/10.1109/jiot.2018.2872122

[10] Hoppe, T., Kiltz, S., & Dittmann, J. (2011, January). Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. Reliability Engineering & System Safety, 96(1), 11–25. https://doi.org/10.1016/j.ress.2010.06.026

[11] Gaussier, E., & Cao, L. (2016, February). Conference Report on 2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA'2015) [Conference Reports]. IEEE Computational Intelligence Magazine, 11(1), 13–14. https://doi.org/10.1109/mci.2015.2502125
[12] Wang, C., Zhao, Z., Gong, L., Zhu, L., Liu, Z., & Cheng, X. (2018). A Distributed Anomaly Detection System for In-Vehicle Network Using HTM. IEEE Access, 6, 9091–9098. https://doi.org/10.1109/access.2018.2799210
[13] Lin, Z.; Shi, Y.; Xue, Z. IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection. arXiv 2018, arXiv:1809.02077.
[14] He, Q., Meng, X., Qu, R., & Xi, R. (2020, August 7). Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles. Mathematics, 8(8), 1311. https://doi.org/10.3390/math8081311
[15] Savitha, P. B., S, M., & S, A. (2023, March). Cyber Security Issues in Connected Autonomous Vehicle. International Journal of Research Publication and Reviews, 4(3), 929–936. https://doi.org/10.55248/gengpi.2023.32358
[16] Shrimant, Gaikwad Vidya, Ravindranath, K. & Prasad, Gudapati Syam(2023) A mathematical model for secure Cloud-IoT communication: Introducing the revolutionary lightweight key mechanism, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1341–1354, DOI: 10.47974/JDMSC-1750
[17] Wanjale, K., Wankhede, D.S., Dongre, Y.V., Mahamuni, M. (2023). Analyzing Machine Learning Algorithm for Breast Cancer Diagnosis. In: Shukla, P.K., Mittal, H., Engelbrecht, A. (eds) Computer Vision and Robotics. CVR 2023. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-99-4577-1_42
[18] Karnik, M.P., Kodavade, D.V. (2023). A Survey on Controllable Abstractive Text Summarization. In: Abraham, A., Pllana, S., Casalino, G., Ma, K., Bajaj, A. (eds) Intelligent Systems Design and Applications. ISDA 2022. Lecture Notes in Networks and Systems, vol 715. Springer, Cham. https://doi.org/10.1007/978-3-031-35507-3_30
[19] Wankhede, D.S., Pandit, S., Metangale, N., Patre, R., Kulkarni, S., Minaj, K.A. (2022). Survey on Analyzing Tongue Images to Predict the Organ Affected. In: , et al. Hybrid Intelligent Systems. HIS 2021. Lecture Notes in Networks and Systems, vol 420. Springer, Cham. https://doi.org/10.1007/978-3-030-96305-7_56
[20] Dr. Selvarani Rangasamy, M. D. S. W. (2021, March 1). REVIEW ON DEEP LEARNING APPROACH FOR BRAIN TUMOR GLIOMA ANALYSIS. INFORMATION TECHNOLOGY IN INDUSTRY, 9(1), 395–408. https://doi.org/10.17762/itii.v9i1.144
[21] Wankhede, D. S., & Selvarani, R. (2022, December). Dynamic architecture based deep learning approach for glioblastoma brain tumor survival prediction. Neuroscience Informatics, 2(4), 100062. https://doi.org/10.1016/j.neuri.2022.100062
[22] Sourav Singh, Manali Bhavsar, Rasika Mahadeshwar, Sumeet Rathod, Mrs.Disha Wankhedw, "PREDICTING IDH1 MUTATION AND 1P19Q CO-DELETION STATUS FOR BRAIN TUMOR". International Journal of Advanced Science and Technology 29(4s):1196-1204.
[23] Mrs. Disha Sushant Wankhede and Dr. Chetan J. Shelke, "An Investigative approach on the prediction of Isocitrate dehydrogenase (idh1) mutations and co-deletion of 1p19q in glioma brain tumors". 22nd International Conference on Intelligent Systems Design and Applications (ISDA'22) December 12-16, 2022 https://link.springer.com/book/10.1007/978-3-030-96308-8 Indexed by: SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago, DBLP, EI Compendex, Japanese Science and Technology Agency (JST), Springer Link
[24] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020, June). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214. https://doi.org/10.1016/j.vehcom.2019.100214
[25] Alkahtani, H., & Aldhyani, T. H. H. (2021, September 9). Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. Security and Communication Networks, 2021, 1–23. https://doi.org/10.1155/2021/3806459
[26] Sadhwani, Sapna, Baranidharan Manibalan, Raja Muthalagu, and Pranav Pawar. 2023. "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques" Applied Sciences 13, no. 17: 9937. https://doi.org/10.3390/app13179937
[27] Oduwole Omolara Oluwakemi , Kene Tochukwu Anyachebelu .(2023) "Comparative Evaluation of MachineLearning Algorithms for Intrusion Detection" Asian Journal of Research in Computer Science DOI: 10.9734/AJRCOS/2023/v16i4366

[28] Arif Hussain Magsi1,* , Ali Ghulam2, Saifullah Memon1, Khalid Javeed3, Musaed Alhussein4 andImad Rida5 (2023)"A Machine Learning-Based Attack Detection and Prevention System in Vehicular Named Data Networking" DOI: 10.32604/cmc.2023.040290

[29] Mishra, V., Kadam, S. (2023). A Systematic Review on Security Mechanism of Electric Vehicles. In: Abraham, A., Pllana, S., Casalino, G., Ma, K., Bajaj, A. (eds) Intelligent Systems Design and Applications. ISDA 2022. Lecture Notes in Networks and Systems, vol 717. Springer, Cham. https://doi.org/10.1007/978-3-031-35510-3_55

[30] Wankhede, D.S., Mishra, V., Honkhambe, A., ...Srivastava, S., George, J. (2022)"An Investigative Study of Plant Disease Prediction using Machine Learning and Deep Learning Algorithms" 13th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2022, 2022, 8, pp. 788–795

[31] Biradar, N., Mohite, Y., Pandey, N., ...Mishra, V., Karnik, M (2022)"Security Challenges in Controller Area Network (CAN) in Smart Vehicles". 13th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2022, 2022, 8, pp. 671–678