Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020936
Article

Tech Science Press

Sensor Data Based Anomaly Detection in Autonomous Vehicles using Modified Convolutional Neural Network

Sivaramakrishnan Rajendar and Vishnu Kumar Kaliappan*

Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, 641407, India
*Corresponding Author: Vishnu Kumar Kaliappan. Email: vishnudms@gmail.com
Received: 15 June 2021; Accepted: 02 September 2021

Abstract: Automated Vehicles (AVs) reform the automotive industry by enabling real-time and efficient data exchange between the vehicles. While connectivity and automation of the vehicles deliver a slew of benefits, they may also introduce new safety, security, and privacy risks. Further, AVs rely entirely on the sensor data and the data from other vehicles too. On the other hand, the sensor data is susceptible to anomalies caused by cyber-attacks, errors, and faults, resulting in accidents and fatalities. Hence, it is essential to create techniques for detecting anomalies and identifying their sources before the wide adoption of AVs. This paper proposes an anomaly detection model using a Modified-Convolutional Neural Network (M-CNN) with Safety Pilot Model Deployment (SPMD) dataset. The M-CNN model comprises specifically trained layers involving the ReLU activation function for feature extraction and detection of AV anomalies. Furthermore, the Adam is used as the optimization algorithm to train the model. The detection accuracy of the proposed model is compared with Isolation Forest (IF) and Support Vector Machine (SVM). The experimental result reveals that the proposed model outperforms the other models with an accuracy of 99.40% in AV anomaly detection.

Keywords: Autonomous vehicle; convolutional neural network; deep learning; feature extraction; anomaly detection

1 Introduction

The latest advancements in connectivity and automation have provided the idea of autonomous vehicle (AV) development. This technology promises to minimize collisions, energy consumption, noise, congestion and increase transportation accessibility. An AV, also known as a Self-Driving Vehicle (SDV), can run and execute required tasks without human interference due to its potential to detect its surroundings. An autonomous vehicle employs a fully automatic driving mechanism to react to environmental situations that a human driver controls. Though the idea of autonomous vehicles is discussed for years, the development costs have hampered large-scale production. Nonetheless, in the last decade, there has been a significant increase in research activities to bring the concept of the AV to reality [1,2]. Further, AVs have advantages such as improved connectivity, mobility, and land use. In addition, AVs can reduce

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

congestion when linked and connected. AV technology has precisely calibrated acceleration-braking maneuvers at all stages to track the local traffic environment regularly and actively. AVs have a significant and long-term effect on land-use patterns [3].

While there can be significant benefits to using AVs, at the same time, there are certain drawbacks that require attention. Ambitious plans for the rapid deployment of fully autonomous vehicles have run into unexpected problems. Among them, stopped fire engines, big white trailers, and highway barriers are a few to mention [4]. Furthermore, the Electrical Vehicle (EV) has certain practical disadvantages, such as restricted distance-travelling capability due to the size and reliability of the batteries [5]. A variety of safety problems has delayed AV production. The safety of AVs has become another major issue for road users, particularly after the recent high-profile collision of the Tesla Model S held in 2016 [6]. While the number of AV accidents has decreased over time, vehicles are even more problematic in the context of crashes that occurred per mile travelled than self-driving cars [7]. Extra safety concerns have arisen due to the mode changes, like disturbance, lack of situational awareness, and heavy workload at take-over. Such aspects are obstacles to the commercial growth of AVs, and they are continuously monitored and resolved. Many citizens also expressed concern about the security risks posed by AVs, like intrusion, fraud, and malicious activities [8–12].

The primary obstacle to the adoption of AVs is insecurity over the job. AVs can replace taxi and bus drivers, delivery people, and anybody who makes money through driving. Also, there is a negative opinion about the AVs, especially the fatalities caused, such as the Uber crash in 2018 [13]. It has been hard to unite coherent legal research. Most of these assess liability in injury situations due to geographical disparities in road traffic and transportation. Among all the barriers mentioned above, the data protection and privacy barriers are significant because the vehicle controls are vulnerable to hacks [14]. The AV starts to roll out due to increased uncertainty regarding privacy and confidentiality. It emerged after implementing the General Data Protection Regulation (GDPR) in 2018 and several problematic data breaches and security issues over the previous seven years. The AV designers still try to compromise both security issues and the requirement of massive data.

People worry that the AVs would potentially be exploited due to the extensive digital technology needed to function. Attackers started explicit usage of the data they have acquired, manipulating the vehicle and allowing it to do actions that the driver is not aware of, not able to reverse, and intentionally harming the member(s) in the vehicle. When cyber-criminals gain control of an automobile, they may inflict minor inconveniences like opening and shutting windows or trigger very severe risks like disrupting the vehicle's skills to process stop signs. The attackers can also maliciously force vehicles to crash and kill their occupants. They can also utilize AVs for terrorist acts like carrying and exploding remote-controlled explosives. Although there is a significant requirement of accountability from carmakers, vehicles may remain more susceptible as a result. Also, there have been few cyber-security problems, as in the London case, in which attackers discover loopholes in AVs using cryptographic ransomware [15]. Such loopholes help attackers steal money from travelers before relinquishing control of the vehicle. These issues must be avoided by strengthening counter-measures.

The proposed work considers the three parameters: speed, vertical acceleration, and GPS to accurately detect the abnormality in the AVs. A Deep Learning (DL) based detection model is used due to its high detection accuracy and extensive data handling capability.

The contributions of this work are summarized as follows:

- A modified convolutional neural network named M-CNN is proposed to detect an anomaly in AV. For extracting features from a raw dataset, five convolution layers are used in M-CNN and following every convolution layer is a max-pooling layer.

- To consider three parameters (speed, vertical acceleration, and GPS) and train the model using a huge data volume to detect instant anomaly type.

The work is organized as follows. Section 2 reviews the related works about anomaly detection in AV. Section 3 describes the proposed method for anomaly detection in AV. Section 4 contains the result and discussion, which shows the efficiency of the proposed work. The conclusion of the research work is discussed in Section 5.

2 Related Works

Han et al. [16] introduced a technique for detecting anomalies in vehicle networks. The anomaly is detected by tracking irregular behavior in the network. The model is designed to identify three common attack types. The authors acknowledged that the proposed approach might identify unknown attacks, but the situations other than these three were not addressed clearly. On the other hand, Rewini et al. [17] suggested a three-layer model (sensing, control and communication) for correctly understanding automotive security attacks. Attacks on the first two layers will spread upward, disrupting performance and risking the control layer's safety. This work doesn't concern with other forms of attacks. Wyk et al. [18] devised a method for detecting and identifying abnormal behaviors in connected and automated vehicles (CAVs) to increase their security. To recognize and predict anomalous behavior in CAVs, they proposed a framework with the help of CNN and the Kalman filter.

He et al. [19] introduced a CAV cyber protection architecture centered on UML (Unified Modeling Language) to describe CAV networks' possible attacks. Depending on the training data, two classification methods were presented. It primarily addressed communication-based threats, and no physical attacks were covered. Few preliminary works have been done to explore future CAV threats. He et al. [20] gathered a wide range of possible cyber-attacks and analyzed them in target properties, threats, and implications. The extent of every category of attack is further evaluated using a newly specified series of parameters. The extent of the attacks may be classified as critical, significant, mild, or minor. Mitigation strategies such as mitigation, elimination, transference, adoption, and contingency planning are further discussed. Park et al. [21] suggested a data analysis approach based on machine learning for detecting suspicious malware activities in massive network traffic in real-time scenarios. They offered a practical approach for identifying malicious activities in a network. Also, tests are performed to validate the proposed method's accuracy by comparing it to other techniques.

Other researches also addressed concrete attacks on CAVs to suggest alternative approaches by use of artificial intelligence and the analysis of possible threats on CAVs. The authors of [22] provided a detailed analysis of recent threats and attacks on CAVs employing machine learning algorithms. Potential threats have been classified as the application layer, system stage, data theft, sensor attack, network layer and so forth. They also highlighted the significance of intrusion detection of cyber-attacks in the growth of CAVs. The authors developed an approach centered on machine learning techniques to identify the position and locate the jamming attack [23]. The anti-jamming system improved vehicular contact efficiency, resulting in higher accuracy and a decreased packet loss ratio. The machine learning relied technique is found to be successful in jamming attacks, mainly on CAV sites.

According to the studies above, unlike cyber protection in other areas, including smartphones, CAV threats can lead to severe consequences for consumers. As per a University of Michigan study [24], the public was most worried about physical harm incurred by CAVs than the leaking of confidential data. Additionally, it is observed that there remains an insufficient amount of related studies for data protection in CAV. The European Defence Agency (EDA) have formally invited proposals for artificial intelligence-based network protection techniques in CAV [25]. For the past few years, Devi et al. [26] reviewed machine learning approaches and methods used to develop autonomous driving systems. Every method's effectiveness is recorded and evaluated in terms of time taken for prediction with accuracy.

Alheeti et al. [27] suggested an intelligent safety system to secure communications in all types of vehicles. Also, the function is built on the Proportional Overlapping Scores approach that enables the amount of features contained in the Kyoto benchmark dataset to be reduced. Guo et al. [28] suggested a new edge computing-based abnormal recognition strategy which employs edge-based sensor data fusion to identify anomalous events. The data from the sensor is used to find when the abnormality occurs inside the vehicle.

Cooperative Adaptive Cruise Control (CACC) in self-driving cars is the focus of Alotibi et al. [29]. They proposed a real-time anomaly detection method based on quantitative learning and kinematics physics rules. They recommended the technique utilized by every vehicle for finding abnormalities, and it depends on the conveyance of individual speed choices. Ryan et al. [30] suggested a new method for quantifying AV injury risks by comparing them to the activities of humans. This proposed technique helps to evaluate the security level of AVs.

Wang et al. [31] suggested a novel observer-based approach for improving connected and autonomous vehicle (CAV) transportation privacy and protection. Model-based signal filtering and abnormality recognition techniques are combined in the proposed process. They used a filter to simplify collected data from a CAV focused on a nonlinear vehicle paradigm. There has been no structured approach in the preceding works to examine the security events of CAVs. Most of the previous works are based on individual generic CAV attacks, such as position-based spoofing assaults or adversarial CAV network assaults. It is also worth noting that there is also a shortage of CAV vulnerability data sets because much analysis has concentrated on theoretical issues, resulting in a lack of detection systems.

The following Tab. 1 shows the technique, dataset, identified attacks, parameters used and efficiency of previous works.

Table 1: Summarization of previous works

Technique [citation]	Dataset	Identified attacks	Parameters used	Efficiency
Survival analysis model [16]	The primary dataset produced by them	Three attack scenarios	–	97% accuracy for three types of attack detection.
Three-layer framework [17]	–	Attack type vary according to each layer type	–	–
Convolutional Neural Network with Kalman filtering [18]	SPMD dataset	Four anomaly types considered	Three sensor values	Accuracy varies according to anomaly type
UML (Unified Modeling Language)-based CAV cyber security method [19]	Generation of CAV-KDD based on KDD99 data set	14 sub attacks were considered	–	Accuracy varies based on attack types

(Continued)

Table 1 (continued)

Technique [citation]	Dataset	Identified attacks	Parameters used	Efficiency
Investigation of potential cyber-attacks [20]	–	Potential cyber-attacks	–	–
Machine learning-based technique [21]	AW & GM dataset	Android based attacks	–	92.9%
An outline of the different problems involved with the use of machine learning in vehicular networks [22]	–	Adversarial ML attacks on CAVs	–	–
Machine based approach [23]	Primary dataset generated by them	External attacks and noise are considered	–	97.25% accuracy
Survey of machine learning algorithms and techniques [26]	–	–	–	–
Intelligent protection mechanism [27]	Kyoto benchmark dataset	External and internal attacks in self-driving vehicles are considered	–	99.18% of training accuracy
Abnormality detection on the basis of edge computing [28]	Primary dataset generated by them	Intrusion attacks	Time domain property and frequency domain property of sensor data	99.5% of true positive rate
Generalised Extreme Studentized Deviate with Sliding Chunks (GESD-SC) technique [29]	–	They identified some of the vital risks as the platoon leader is being hacked and modifies acceleration details transmitted to platoon associates	Speed and acceleration data	Accuracy is 89.7% when chunk size is 5. Accuracy is 92.8% when chunk size is 20
Convolutional Neural Networks (CNN) [30]	Primary dataset generated by them	–	Steering angles and velocity	–
One Class Support Vector Machine (OCSVM) [31]	Primary dataset generated by them	Sensor anomalies	Vehicle's on-board sensors values	–

3 Materials and Methodology

3.1 Dataset

The data used in this paper is from the Research Data Exchange (RDE) archive for the Safety Pilot Model Deployment (SPMD) [32]. The key aim of this programme is to show autonomous vehicles in real-world scenarios, emphasizing networking systems such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The data is gathered with high accuracy and frequency over 2,500 vehicles in two years.

In the feature extraction process, this SPMD data is given as input to the model. The features extracted are vehicle speed, GPS speed, and vehicle acceleration. Out of three extracted features, the first two refer to the test vehicle's speed, and the third feature is used to conclude speed containing 2,980 s of trip length. The dataset is produced with anomalies through simulation in this work. It is due to the lack of datasets for CAVs that provides sensor measurement with variations induced by attacks or defects and ground realities. In particular, this work takes into account an instant anomaly. An instant anomaly is a sudden change in these data values. Also, the model is not trained when there is a fault or complete attack in sensors of AV. The instant anomaly type is injected randomly into the dataset for training the model. The anomalies are simulated with the randomly selected period to the dataset. Finally, the generated anomalies are added to the original dataset.

3.2 Training and Testing Dataset

The dataset is split into two groups with 80% training data and 20% testing data concerning common rules in neural networks. By using the training dataset, models are trained, and predictions are carried out on the test dataset. Moreover, 80% of data are taken as training data and 10% as validation data from the training dataset for determining the model's performance, loss, precision, and recall. For both training and testing, the collected data is preprocessed to remove noise. The training step includes hyperparameter optimization and anomaly detection. The hyperparameter includes learning rate = 0.001 and the number of epoch = 100, batch size = 64. The proposed model is trained using these parameters. Also, for accurate results, the model is trained using Adam optimizer.

3.3 Workflow

This section presents the workflow of the proposed model. It consists of data preprocessing, feature extraction from the SPMD dataset and anomaly detection from the extracted features. Next, anomaly detection is done based on a DL approach. Convolutional Neural Network (CNN) approach is considered to carry out anomaly detection, and then layers are altered to achieve accurate results. The anomaly in AV can be detected at the output of the last layer in M-CNN. Next, the machine learning models are discussed. Fig. 1 shows the anomaly detection in AV using ML and DL based models.

3.4 Anomaly Detection in AV Using Machine Learning Models

Several machine learning models have been used in recent days for anomaly detection in AV. Among them, Isolation forests and SVM perform well. When compared to these two models, the proposed M-CNN performs better.

3.4.1 Isolation Forest

Isolation forest comes under the category of unsupervised learning algorithm, which is mainly used in anomaly detection [33]. It operates on the concept of isolating anomalies rather than the most traditional techniques of profiling regular points. It identifies irregularities in data through the isolation of outliers. The benefit of using the isolation forest is that it identifies abnormalities quicker and consumes low memory than other anomaly detection methods.

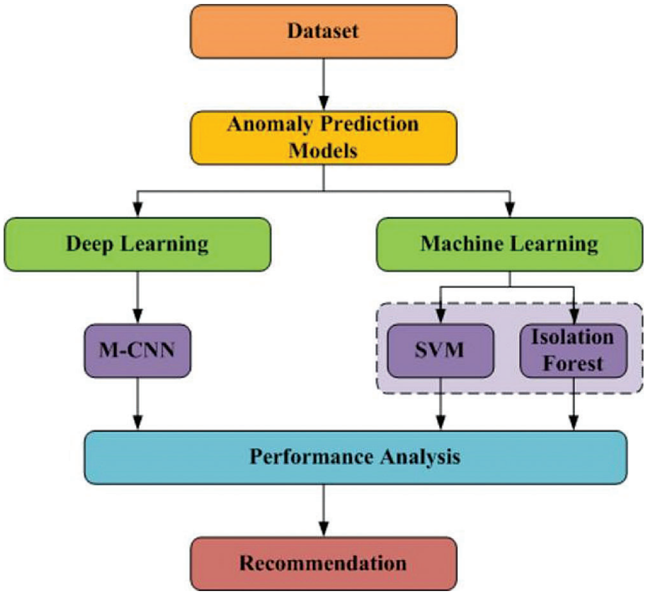


Figure 1: Flow of the proposed model

The isolation forest algorithm is based on the decision tree algorithm. This separates outliers by simply choosing a feature from the specified set of features and then choosing a partition value for the selected features. This random feature separation may result in narrower paths in trees for abnormal data values, separating it from the usual data collection.

3.4.2 SVM

Support Vector Machine (SVM) is often used in detection and classification problems since it belongs to a supervised machine learning algorithm. SVMs use hyperplanes in multi-dimensional space to separate one class of observations from another. Naturally, SVM is used in solving multi-class classification problems [34]. On the other hand, SVM is progressively being used in one class problems in which all data belong to a single class. In this scenario, the algorithm is given the training to learn, which is normal. After that, the algorithm is given new data to identify whether it should belong to the group. If not, the latest data is labelled as out of ordinary or anomaly.

3.5 Anomaly Detection in AV Using m-CNN

Anomaly in AVs can be detected using a Modified Convolutional Neural Network named M-CNN. Firstly, the features are extracted from raw data, and then an anomaly detection in AV is carried out. In the proposed M-CNN, the feature extraction is carried out in convolutional and pooling layers. Then anomaly is detected in the fully connected layer of CNN, and this flow is shown in Fig. 2.

During the initial screening process, some of the redundant features are seen in the raw dataset. These features cause processing overhead and are not helpful during attack detection. So the most promising and valuable features are extracted from the dataset using the proposed model. The proposed CNN model consists of five convolution layers and maximum pooling layers. The main components M-CNN are as follows:

- Input layer
- Convolution layers
- Max-pooling layers
- Fully connected layer
- Output layer

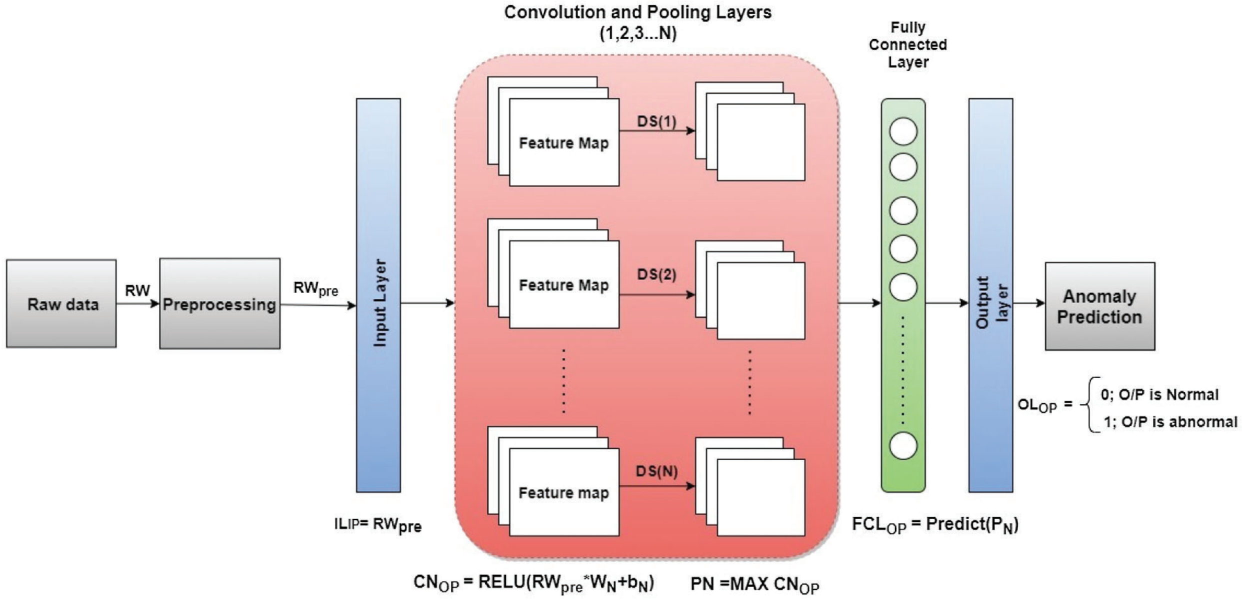


Figure 2: Anomaly detection in AV using DL based M-CNN

3.5.1 Preprocessing

The preprocessing is initially carried out before passing the raw data (RW) from the dataset to the input layer. This preprocessing step removes the null data from the raw input dataset. Also, it eliminates noise and duplicate values from RW. The preprocessed output *RWpre* can be given as,

$$\begin{aligned} Preprocess(RW) = RWpre = Denoise(RW) + \text{eliminate\_}Null(RW) \\ + De\_duplicate(RW) \end{aligned} \tag{1}$$

3.5.2 Input Layer

The preprocessed data *RWpre* is given as input to the input layer. This process can be denoted using below Equation,

$$IL_{IP} = f(RW_{pre}) \tag{2}$$

3.5.3 Convolution Layers

The most significant layer used for feature extraction in CNN is the convolution layer. This layer derives the most prominent features from the data of the previous input layer. This convolutional layer contains learnable kernels or filters used in the feature extraction process. The one-dimensional feature maps are generated by carrying out a convolutional operation over the input data in this convolution layer by M-CNN. Using multiple kernels over this layer, different features can be extracted from *RWpre*. The particular features are detected on all the locations in this layer's input feature map by the kernel. This helps in weight sharing in the feature map. This feature of local networking and weight-sharing efficiently decreases complications in the network and the amount of training parameters. There are N convolutional layers (C_1, C_2, $C_3 \ldots C_N$) used for process of feature extraction. In this work, N = 5, which means 5 convolutional layers are used. The filters used in convolution layers are 2 × 2. In each convolutional layer, kernel slides come over input to produce a feature map.

The Nth convolutional layer output can be defined as [35],

$$CN_{OP} = ReLU(RW_{pre} * \ W_N + b_N) \tag{3}$$

where CN_{OP} denotes the output of Nth convolution layer; $RWpre$ denotes the input data; W_N and b_N denotes weight and bias of the Nth layer. After the convolution operation, the ReLU activation function is applied to the result.

After this operation, neurons are activated using Rectified Linear Unit (ReLU). This ReLU is important in the neural network, where input in the network node is converted to output. It permits the neural network to learn nonlinear dependencies and mitigate vanishing gradients with a better learning rate. Also, it has a faster convergence rate. Generally, linear activation functions are used in the output layer for predictions in networks.

The ReLU function with input vector x can be expressed as,

$$ReLU\ (x) = \max\ (0,\ \ x) \tag{4}$$

3.5.4 Max-pooling Layers

Each convolution layer is accompanied by a pooling layer in CNN. The input for this pooling layer will be the output of the previous convolution layer. Here N = 5 and the pooling layers are denoted as (P_1, P_2, $P_3 \ldots P_N$). Generally, pooling comes under two categories such as max pooling and average pooling. Noise can be suppressed using this max-pooling layer. It can eliminate the noise activations as well as carry out de-noising and dimensionality reduction. In comparison, the average pooling conducts dimensionality reduction as a noise suppression process. Hence max-pooling performs better than average pooling. The resulting output from the previous convolutional layer is transferred to this max-pooling layer, which performs down sampling on the feature map in this max-pooling layer. The extracted features from the dataset in this layer are speed, vertical acceleration and GPS.

The pooling layer output can be denoted as [35],

$$P_N = \max_{N \in S} CN_{OP} \tag{5}$$

where P_N denotes the pooled feature map. S is the pooling region in the feature map.

3.5.5 Fully Connected Layer

This model is trained based on extracted features in the previous layer. Using the trained model, the anomaly presented in AV is detected in this layer. The training loss and error rate has been reduced in proposed M-CNN when compared to other existing methods. The fully connected layer output can be denoted as,

$$FCL_{OP} = Predict(P_N) \tag{6}$$

3.5.6 Output Layer

This is the last layer in the proposed M-CNN, and it gives whether the anomaly is presented in the proposed work or not. The final output $OLOP$from this layer can be denoted as,

$$OL_{OP} = \begin{cases} 0, & if\ OP\ is\ Normal \\ 1, & if\ OP\ is\ abnormal \end{cases} \tag{7}$$

The output will be 0 if there is no anomaly in AV, and the output will be 1 when it is present. If an anomaly presented in the AV is detected, immediate action will be taken before the vehicle loses its complete control.

Adam optimization

The optimization algorithm used in this work is Adam and it helps for weight updation using training data. This Adam optimization utilizes the benefits from Adaptive Gradient (AdaGrad) algorithms and Root Mean Square Propagation (RMSProp) algorithms. It computes the individual adaptive learning rate for each parameter θ.

The exponentially decaying average of past gradients *mi* are used by Adam optimizer, and it is same as same as momentum [36]:

$$V_i = \beta_1 V_{i-1} + (1 - \beta_1)g^2 i \tag{8}$$

$$m_i = \beta_2 m_{i-1} + (1 - \beta_2)g_i \tag{9}$$

In Eqs. (5) and (6), *Vi* denotes the variance and *mi* represents the mean values.

Adam updated rule can be represented as follows by the use of these variables,

$$\phi_{i+1} = \theta_i \frac{\mu}{\sqrt{v_i + \varepsilon}} \tag{10}$$

This optimization method updates weights, and the correct learning rate is chosen for accurate prediction.

4 Results and Discussion

The experiment is performed on Intel Core i7 3.5 GHz processor machine with NVIDIA GPU enabled 4 GB RAM. The DL frameworks like Keras are used for implementing the model using Python. Recently, CNN models have been used in diverse fields to solve problems such as anomaly detection and classification. The DL based M-CNN (DL-MCNN) model is presented in this work for detecting anomalies in the AV. To increase accuracy, the DL-MCNN model is trained using instant anomaly type as well as the hyperparameters are optimized with the help of a DL technique. A confusion matrix is used to assess the proposed work's performance on the test data.

In the confusion matrix, the rows provide the information about the true class, and the columns give information on the predicted class. This matrix contains four outputs: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

TP signifies that if the result is positive and therefore it corresponds to the positive class category. TN indicates that if the result is negative, so it corresponds to the negative class category. FP indicates that if the result is negative, so it corresponds to the positive class category. If FN indicates that the result is negative, so it corresponds to the negative class category. Due to class variations and the amount of data sets, the number of FPs and FNs varies by class. Fig. 3 shows the proposed model's confusion matrix for detecting anomalies using the Adam optimizer. At each point on the test dataset, the confusion matrix can be used to calculate the TP, TN, FP, and FN norms.

The detection accuracy of the proposed M-CNN achieves a detection accuracy of 98%. We have taken 50,000 data from the SPMD dataset. Out of this, 8000 data values are used for testing, 42,000 data for training the data. In the confusion matrix, TP value = 2573, which shows the model correctly predicts the anomaly in AV as an anomaly. TN = 480, which shows the model correctly predicts that there is no anomaly in AV. Similarly, the FN = 6799, which shows the model correctly predicts no anomaly in AV. FP = 148, which shows the model incorrectly predicts that there is an anomaly in AV. The confusion matrix is used to calculate these TP, TN, FP, and FN values.

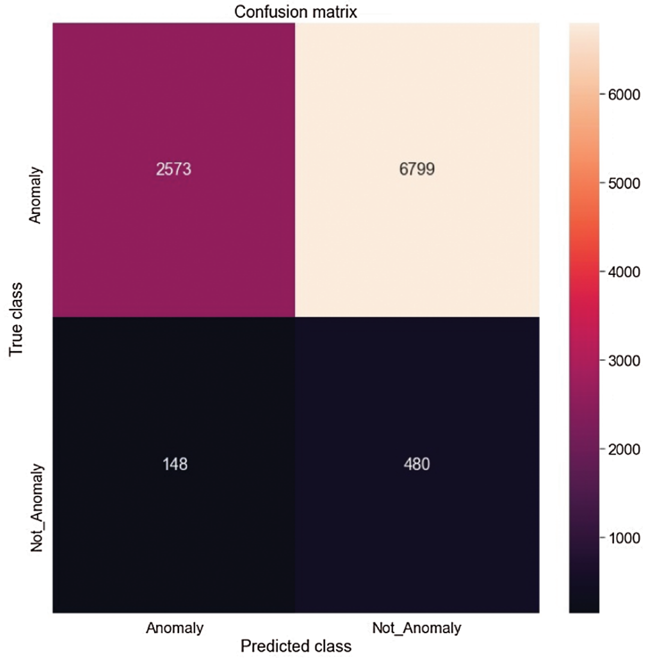


Figure 3: Confusion matrix for the proposed M-CNN

The Receiver Operator Characteristic (ROC) curve seems to be an important metric for classifying and identifying problems. This ROC is a probability curve that is used to plot the True Positive Rate (TPR) across the False Positive Rate (FPR) over various threshold levels in order to distinguish the signal from the noise. TPR also called as sensitivity indicates how much of the negative class is accurately estimated. The FPR, or specificity shows us how much of the negative class is wrongly estimated by the model. The Area Under the Curve (AUC) is an indicator of a model's capability to differentiate between groups as well as it is used to summarize the ROC curve. In this paper, AUC = 0.5338, and it is a high value indicating that the model's output in dividing between positive and negative groups is higher.

In Fig. 4, the ROC curve closer towards the top left corner which indicates the proposed work accurately detect the anomaly in AV when compared to the existing work.

From Tab. 2, the true positive rate for the proposed M-CNN is high compared to other existing methods like isolation forest and SVM. It is clear that the proposed method correctly identify the high number of anomalies and a low number of false positives. The proposed M-CNN correctly detects the anomalies because the model is given robust training with a large amount of data. The null values are eliminated in preprocessing stage before training.

Based on the confusion matrix on the test dataset, this precision-recall curve is drawn. The M-CNN has a high AUC value, and it indicates the model is returning accurate results (high precision) and a majority of positive results (high Recall). Precision is defined as the amount of positive samples correctly labelled to the total number of positive samples classified (either correctly or incorrectly). The precision metric assesses the model's ability to interpret a result as positive accurately. Precision values vary from 0 to 1.

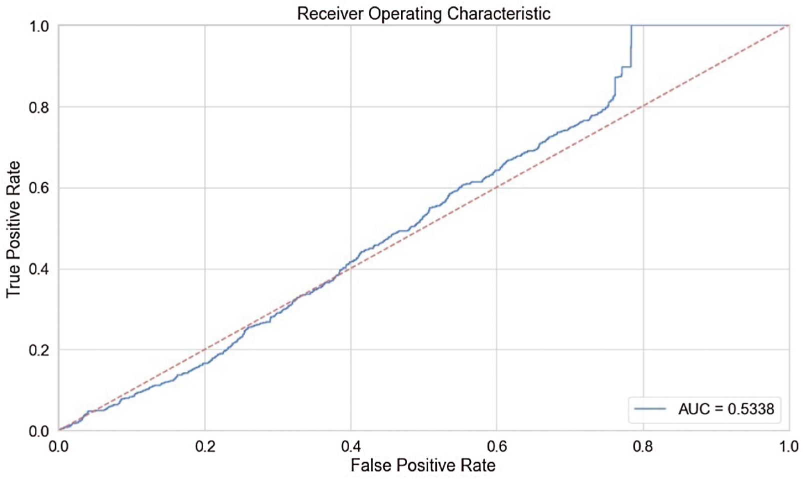


Figure 4: ROC graph for proposed M-CNN

Table 2: ROC curve for proposed M-CNN and existing models

False positive rate	True positive rate		
	Proposed M-CNN	Isolation forest	SVM
0.0	0.0	0.0	0.0
0.2	0.18	0.16	0.14
0.4	0.42	0.39	0.37
0.6	0.64	0.62	0.59
0.78	0.9	0.87	0.85

The precision [36] can be denoted as,

$$Precision = \frac{True_{Positive}}{True_{Positive} + False_{Positive}} \tag{11}$$

In anomaly detection, a false positive means that an Av is not under attack (actual negative) has been identified as under attack (predicted anomaly). The AV loses complete control over the attacker if the precision is not high for the anomaly detection model. The recall is used to determine the number of accurate positive predictions by calculating the number of true positive results to total samples.

The recall can be denoted as [36]:

$$Recall = \frac{True_{Positive}}{True_{Positive} + False_{Negative}} \tag{12}$$

Figs. 5a and 5b show the comparison accuracy, and precision and recall values of proposed M-CNN with existing models such as IF and SVM, respectively.

The higher the recall, the higher the accurate anomaly detection. The five convolutional and max-pooling layers are utilized for extracting prominent features. This results in more accurate training, which results in more precise detection accuracy. The proposed M-CNN achieves a precision value of 97.1%, higher than existing models indicating the proposed method's better performance. Moreover, the proposed M-CNN reaches a recall value of 98.7%, which is higher than existing models, showing the proposed method's better performance.

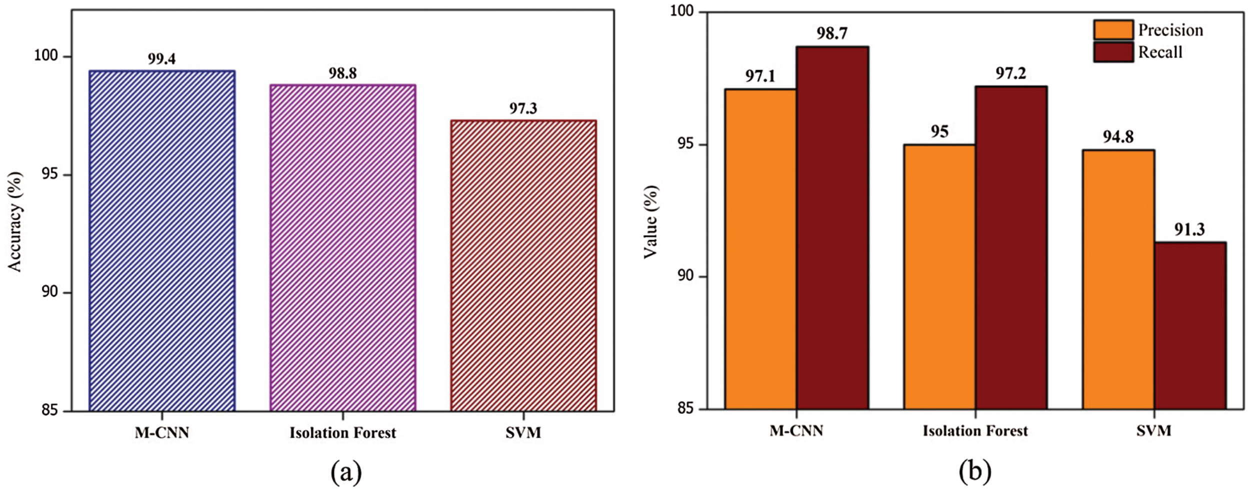
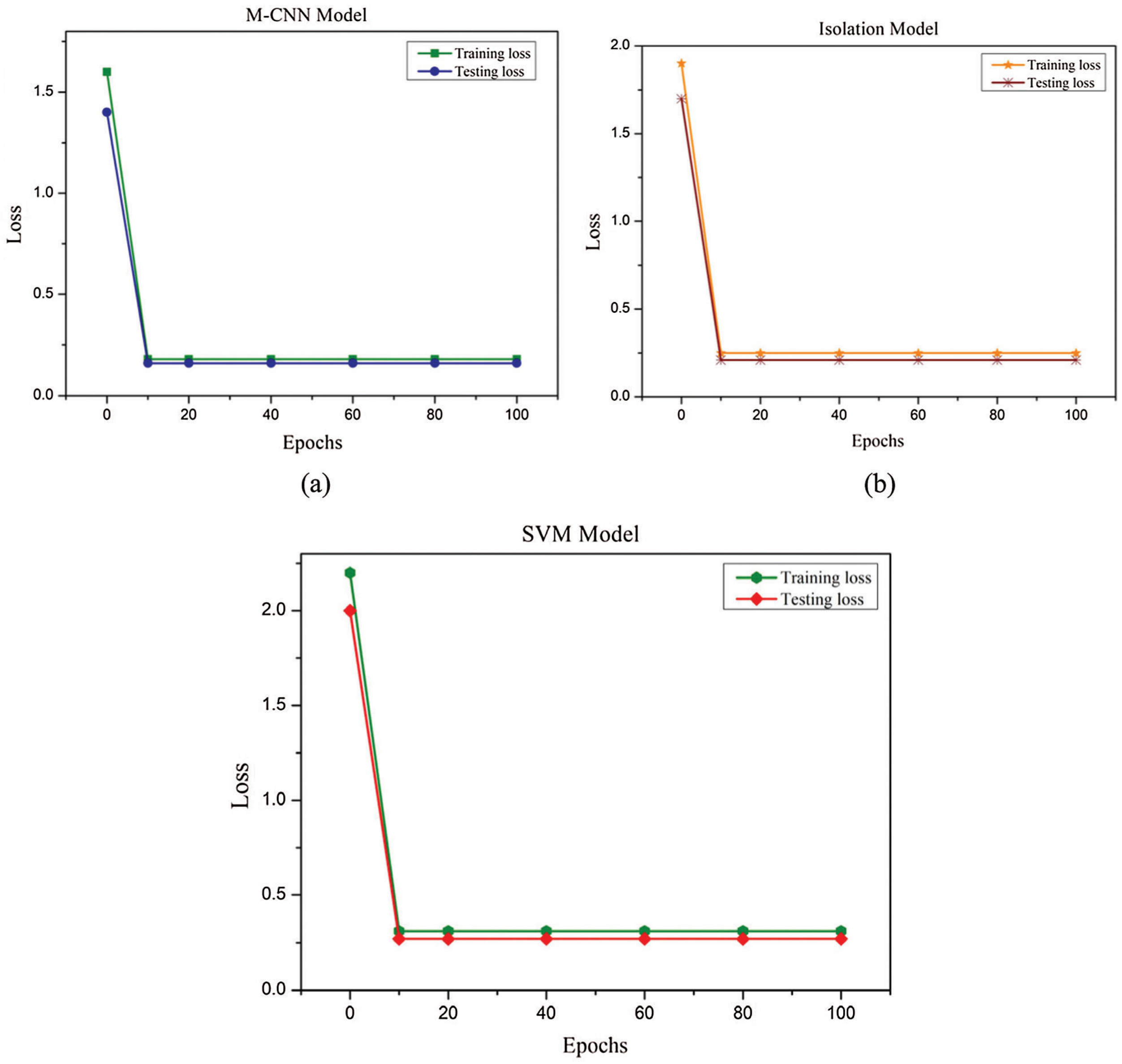


Figure 5: (a) Accuracy comparison of M-CNN with IF and SVM (b) Comparison of precision and recall of M-CNN with IF and SVM

The loss function is one of the important components of neural networks, and it is a prediction error of the model. The dataset is divided into two groups, as stated in Section 3.2. Train data is used to train the model. Later, during the detection of an anomaly in AV, test data is used. Model loss is calculated at both of these stages. The model loss on the training and test dataset for M-CNN is illustrated in Fig. 6a. This shows the model loss for epochs = 100. By modifying the weight vector values and utilizing the Adam optimization method, the value of loss function value is reduced with regard to the model's parameters in this paper. Figs. 6b and 6c indicate the model loss of isolation forest and SVM. The training loss and training loss of these two methods are higher than the proposed M-CNN. Due to proper training with a large dataset, the proposed M-CNN has low test loss compared to existing models.

Tab. 3 shows the 15 sample values from the dataset for attack detection in AV. It consists of three parameters such as speed, GPS_time and lateral acceleration values from AV. The instant anomaly in AV is detected since there is a sudden large change in these three data values.

Fig. 7a shows the attack detection in AV using GPS_time, and Fig. 7b shows the attack detection in AV using speed and lateral acceleration (lateral_acc). The abnormal behavior of the AV is identified since there is a significant change in these three values. Also, the proposed M-CNN accurately detects anomalous behavior since it extracts the essential features from the dataset. The values of these three parameters drop suddenly and become stable after a period. Then, after a specific interval, a quick rise of these parameters is observed. This sudden change indicates an anomaly, and AV is at risk and loses its control.



(a)

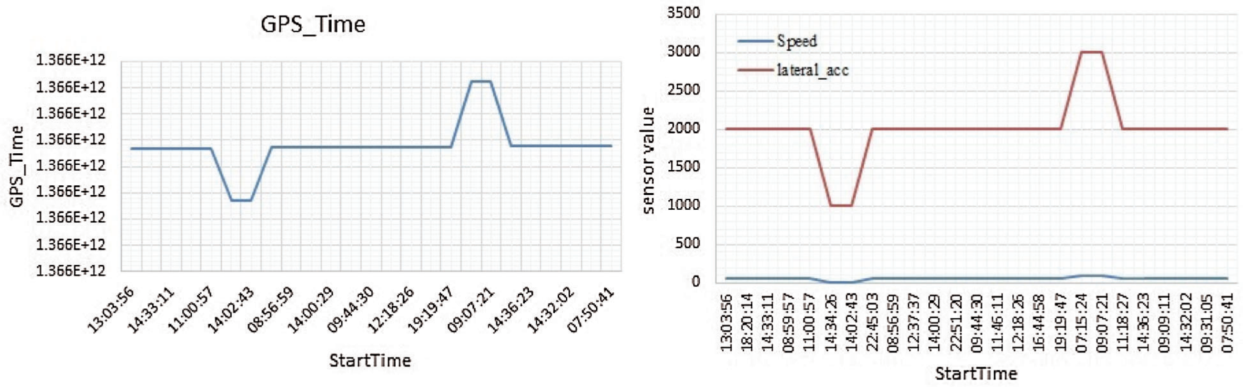
(b)

(c)

Figure 6: (a) Training and testing loss comparison M-CNN (b) Training and testing loss comparison IF (c) Training and testing loss comparison SVM

Table 3: Attack detection using 15 sample values

Start time	Speed	GPS_time	Lateral_acc
13:03:56	50.904	1.36605777330E + 12	2001
18:20:14	51.696	1.36605777350E + 12	2001
14:33:11	51.408	1.36605777360E + 12	2001
08:59:57	51.48	1.36605777370E + 12	2001
11:00:57	51.48	1.36605777370E + 12	2001
14:34:26	11.264	1.36605773410E + 12	1001
14:02:43	11.264	1.36605773410E + 12	1011
22:45:03	51.336	1.36605777420E + 12	2001
08:56:59	51.336	1.36605777420E + 12	2001
12:37:37	50.76	1.36605777440E + 12	2001
14:00:29	50.688	1.36605777450E + 12	2001
22:51:20	49.896	1.36605777460E + 12	2001
09:44:30	49.68	1.36605777470E + 12	2001
11:46:11	49.68	1.36605777470E + 12	2001
12:18:26	51.048	1.36605777490E + 12	2001



(a) (b)

Figure 7: (a) Attack detection using GPS_time (b) Attack detection using speed and lateral_acc

5 Conclusion

Anomaly detection is a vital step in AV development to ensure safety and security. The anomalies in the sensor data must be precisely detected, as cyberattacks, errors, or faults might cause them. This paper proposed a DL-based M-CNN model that enables AVs to detect anomalies in onboard and external sensor data. The results show that the proposed model improves the anomaly detection rate even when the dataset has minimal abnormal cases. Moreover, the DL models with extensive training enable the model to attain a higher detection rate than other existing models on the SPMD dataset. The proposed M-CNN with Adam optimizer achieves a detection accuracy of 99.40%, which is 10% greater than the existing models. Furthermore, the performance of the M-CNN model is evaluated in terms of ROC, AUC, precision and recall. The M-CNN attains 97.10% and 98.70% precision and recall, respectively, which is comparatively higher than the IF and SVM models. While the present model contributes towards detecting instant anomalies in AVs, detecting the other AV attacks on a real-world dataset is significant future research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, pp. 167–181, 2015.

[2] The Welding Institute (TWI)–Global Company, *What is an autonomous vehicle?*, Joining Innovation with Expertise–TWI, 2018. [Online]. Available: https://www.twi-global.com/technical-knowledge/faqs/what-is-an-autonomous-vehicle.

[3] S. A. Bagloee, M. Tavana, M. Asadi and T. Oliver, "Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies," *Journal of Modern Transportation*, vol. 24, no. 4, pp. 284–303, 2016.

[4] J. Hecht, *Self-driving vehicles: Many challenges remain for autonomous navigation*, Laser Focus World, 2020. [Online]. Available: https://www.laserfocusworld.com/test-measurement/article/14169619/selfdriving-vehicles-many-challenges-remain-for-autonomous-navigation.

[5] B. Schoettle and M. Sivak, "Potential impact of self-driving vehicles on household vehicle demand and usage," *Transportation Research Institute*, vol. UMTRI-2015-3, pp. 1–14, 2015.

[6] S. Jack, "Machine learning, social learning and the governance of self-driving cars," *Social Studies of Science*, vol. 48, no. 1, pp. 25–56, 2017.

[7] M. Ryan, "The future of transportation: Ethical, legal, social and economic impacts of self-driving vehicles in the year 2025," *Science and Engineering Ethics*, vol. 26, pp. 1185–1208, 2020.

[8] K. Othman, "Public acceptance and perception of autonomous vehicles: A comprehensive review," *AI Ethics*, vol. 1, pp. 355–387, 2021.

[9] A. R. Javed, Z. Jalil, S. A. Moqurrab, S. Abbas and X. Liu, "Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. e4088, pp. 1–18, 2020. https://doi.org/10.1002/ett.4088.

[10] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, pp. 4291–4300, 2020.

[11] J. Terken and B. Pfleging, "Toward shared control between automated vehicles and users," *Automotive Innovation*, vol. 3, no. 1, pp. 53–61, 2020.

[12] T. M. Hoang, N. M. Nguyen and T. Q. Duong, "Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and K-means clustering," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 139–142, 2020.

[13] Ellen P. Goodman, "Self-driving cars: Overlooking data privacy is a car crash waiting to happen," The Guardian, 2016. [Online]. Available: https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security.

[14] S. Levin and J. C. Wong, "Self-driving uber kills arizona woman in first fatal crash involving pedestrian," The Guardian, March 19, 2018, https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe.

[15] J. Bowles, "Autonomous vehicles and the threat of hacking," *CPO Magazine*, 2019. [Online]. Available: www.cpomagazine.com/2018/10/01/autonomous-vehicles-and-the-threat-of-hacking/.

[16] M. L. Han, B. I. Kwak and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," *Vehicular Communications*, vol. 14, pp. 52–63, 2018.

[17] Z. E. Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, pp. 100214, 2020.

[18] F. V. Wyk, Y. Wang, A. Khojandi and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 1264–1276, 2020.

[19] Q. He, X. Meng, R. Qu and R. Xi, "Machine learning-based detection for cyber security attacks on connected and autonomous vehicles," *Mathematics*, vol. 8, no. 8, pp. 1311, 2020.

[20] Q. He, X. Meng and R. Qu, "Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles," *Journal of Advanced Transportation*, vol. 2020, pp. 1–15, 2020.

[21] S. Park and J. Y. Choi, "Malware detection in self-driving vehicles using machine learning algorithms," *Journal of Advanced Transportation*, vol. 2020, pp. 1–9, 2020.

[22] A. Qayyum, M. Usama, J. Qadir and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the Way forward," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 998–1026, 2020.

[23] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao *et al.*, "Delimitated anti jammer scheme for internet of vehicle: Machine learning based security approach," *IEEE Access*, vol. 7, pp. 113311–113323, 2019.

[24] M. Sivak and B. Schoettle, *Cybersecurity concerns with self-driving and conventional vehicles*, The University of Michigan, Sustainable Worldwide Transportation, vol. SWT-2017-3, pp. 1–13, 2017.

[25] ESA Space Solutions, Cyber security and space based services—ESA business applications, 2019. [online]. Available: https://business.esa.int/funding/invitation-to-tender/cyber-security-and-space-based-services.

[26] S. Devi, P. Malarvezhi, R. Dayana and K. Vadivukkarasi, "A comprehensive survey on autonomous driving cars: A perspective view," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2121–2133, 2020.

[27] K. M. A. Alheeti and K. M. Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles," *Systems Science & Control Engineering*, vol. 6, no. 1, pp. 48–56, 2018.

[28] F. Guo, Z. Wang, S. Du, H. Li *et al.*, "Detecting vehicle anomaly in the edge via sensor consistency and frequency characteristic," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5618–5628, 2019.

[29] F. Alotibi and M. Abdelhakim, "Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3468–3478, 2021.

[30] C. Ryan, F. Murphy and M. Mullins, "End-to-end autonomous driving risk analysis: A behavioural anomaly detection approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1650–1662, 2021.

[31] Y. Wang, N. Masoud and A. Khojandi, "Real-time sensor anomaly detection and recovery in connected automated vehicle sensors," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1411–1421, 2021.

[32] D. Bezzina and J. Sayer, *Safety Pilot Model Deployment: Test Conductor Team Report*. Washington, DC, USA: U. S. Dept. Transp., Tech. Rep. DOT HS 812, 2014.

[33] F. T. Liu, K. M. Ting and Z. H. Zhou, "Isolation forest," *Eighth IEEE International Conference on Data Mining*, vol. 2008, pp. 413–422, 2008.

[34] M. Alam, "Support vector machine (SVM) for anomaly detection," Medium. Retrieved from https://tinyurl.com/26jc6jme*, February 9, 2021.*

[35] L. Jing, M. Zhao, P. Li and X. Xu, "A convolutional neural network based feature learning and fault diagnosis method for the condition monitoring of gearbox," *Measurement*, vol. 111, pp. 1–10, 2017.

[36] R. Thangaraj, S. Anandamurugan and V. K. Kaliappan, "Automated tomato leaf disease classification using transfer learning-based deep convolution neural network," *Journal of Plant Diseases and Protection*, vol. 128, no. 1, pp. 73–86, 2020.