IIDS: Intelligent Intrusion Detection System for Sustainable Development in Autonomous Vehicles

Sudha Anbalagan, Gunasekaran Raja, *Senior Member, IEEE*, Sugeerthi Gurumoorthy, R. Deepak Suresh, and Kapal Dev, *Senior Member, IEEE*

***Abstract*— Connected and Autonomous Vehicles (CAVs) enable various capabilities and functionalities like automated driving assistance, navigation and path planning, cruise control, independent decision making, and low-carbon transportation in the real-time environment. However, the increased CAVs usage renders the potential vulnerabilities in the Internet of Vehicles (IoV) environment, making it susceptible to cyberattacks. An Intrusion Detection System (IDS) is a technique to report network assaults by potential Autonomous Vehicles (AVs) without encryption and authorization procedures for internal and external vehicular communications. This paper proposes an Intelligent IDS (IIDS) to enhance intrusion detection and categorize malicious AVs using a modified Convolutional Neural Network (CNN) with hyperparameter optimization approaches for IoV systems. The proposed IIDS framework works in a 5G Vehicle-to-Everything (V2X) environment to effectively broadcast messages about malicious AVs. Thus IIDS aids in preventing collisions and chaos, enhancing safety monitoring in the traffic. The experimental results depict that the proposed IIDS achieves 98% accuracy in detecting attacks.**

***Index Terms*— Deep learning, autonomous vehicles, intrusion detection, safety monitoring, IoV, 5G-V2X.**

I. Introduction

THE rapid rise of the Internet of Things (IoT) and Internet of Vehicles (IoV) technologies have transformed network-controlled Autonomous Vehicles (AVs) into Intelligent Transportation Systems (ITS) [1], [2]. The Controller Area Network (CAN) is the primary unit for the In-Vehicle Network (IVN), leading to the sustainable development of AVs in the real-time environment. CAN allows communication among Electronic Control Units (ECUs) to conduct operations and adopt functionalities [3]. Increased automobile network connectivity, accessibility and utilizing External Vehicular Networks (EVNs) have also raised the cyberattack surfaces for modern vehicles. Furthermore, due to the limited interval of CAN packet transmission, no authentication or encryption mechanisms are employed during processing. Hence cyber attackers can easily inject malicious messages into IVNs and EVNs to conduct various attacks, such as Denial of Service (DoS), fuzzy, and spoofing. These cyberattacks are often designed to gain access, modify motor control, deny necessary data transmission, or disrupt legitimate AV activities [4]. As a result, developing an Intrusion Detection System (IDS) to detect assaults on IoV systems and AVs is essential.

Connected and Autonomous Vehicles (CAVs) require enhanced management, administration, communication, data storage, and decision-making speed [5], [6]. These characteristics become more critical when a coordinated operation of many CAVs is envisaged. Thus, collaborative and intelligent decision making is required by employing sophisticated Machine Learning (ML) algorithms. In reality, CAVs are vulnerable to all types of classical cyberattacks. Moreover, the impact will be higher since CAVs rely primarily on systems that employ Artificial Intelligence (AI) techniques to make decisions without a driver [7].

ML offers enormous possible solutions to various issues raised by the massive data produced by CAVs [8]. It has significant potential with the various challenges caused by the massive real-time data that CAVs generate and other cutting-edge technological systems such as IoT and Cyber-Physical Systems (CPS) [9]. At the same time, Deep Learning (DL) algorithms enable an intelligent analysis of complex datasets to uncover patterns with minimal human intervention. Thus DL is crucial for the operation of CAVs and other autonomous devices that enable decision-making in coordination.

According to the US National Institute of Standards and Technology (NIST), faster data transmission also significantly determines the effectiveness of such CPS and smart security. Advanced networking technologies are crucial determinants for AVs with runtime aid and advanced security measures. Fifth Generation (5G) Vehicle-to-Everything (V2X) communication tends to be one of the cutting-edge technologies providing greater bandwidth occupying many users. Thus 5G-V2X allows better connectivity to the CAVs in the dynamic IoV environment so the broadcasted alert message can easily reach the peer AVs maintaining smooth traffic [10], [11].

This paper proposes an Intelligent Intrusion Detection System (IIDS) hosted on a 5G-V2X environment to increase swiftness and accuracy in dealing with intrusion detection

Manuscript received 14 October 2022; revised 1 March 2023; accepted 10 April 2023. The Associate Editor for this article was Z. Lv. *(Corresponding author: Sudha Anbalagan.)*

Sudha Anbalagan is with the Centre for Smart Grid Technologies, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India (e-mail: sudha.a@vit.ac.in).

Gunasekaran Raja and R. Deepak Suresh are with the NGN Lab, Department of Computer Technology, Anna University, MIT Campus, Chennai 600044, India (e-mail: dr.r.gunasekaran@ieee.org; deepaksuresh1406@gmail.com).

Sugeerthi Gurumoorthy is with Citicorp Services Pvt. Ltd., Chennai 600113, India (e-mail: sugeerthiguru@gmail.com).

Kapal Dev is with the Department of Institute of Intelligent Systems, University of Johannesburg, Johannesburg 2006, South Africa (e-mail: kapal.dev@ieee.org).

Digital Object Identifier 10.1109/TITS.2023.3271768

in AVs. This framework can prevent many new age attacks and mitigate the vehicular network's total catastrophic failure.

The main contributions of the paper are listed below:

1) A novel IIDS framework is proposed for efficient cyber-attack detection in the IVN and EVN by employing a data transformation approach that effectively transforms vehicle network traffic data into images for the facile differentiation of distinct cyberattack patterns.
2) Malicious AVs are classified into distinct categories by modified Convolutional Neural Network (CNN) with hyperparameter optimization. These malicious AVs are forced to slow down and isolate themselves from the network. Once the vulnerable behavior is resolved, the AVs are gradually reintegrated into the network, ensuring the fidelity and efficiency of IIDS framework.
3) To avoid catastrophic failure in the IoV environment, the IIDS framework employs a decentralized 5G-V2X network that enables several AVs to detect cyberattacks by transmitting alarm messages, resulting in fast and reliable intrusion detection.

The rest of this paper is structured as follows. Section II consists of the existing contributions. The vulnerabilities of the vehicular networks are presented in Section III. Section IV presents the system model. Section V explains the proposed intelligent intrusion detection system. Section VI includes an analysis of the findings. Finally, Section VII draws the conclusion and future work for this article.

II. Related Works

Enabling safety and security for AVs and pedestrians in the IoV environment has become a primary concern. Identifying assaults in vehicular networks is crucial to prevent severe consequences due to the abnormal behavior of malicious AVs. Researchers propose a revolutionary box-plot method [3] premised on a scoring system to sort raw information from actual AVs based on statistical analysis. Ultimately, the clock skews are calculated and combined to build a linear model of the transmitter ECU. It illustrates the efficacy of this strategy in protecting the CAN bus against a masquerade attack. An adaptive synchronization-based control algorithm and collaborative anomaly detection system protect AVs from malicious activities and aid in the lane-following mechanisms in a distributed manner [12], [13]. Although, the scoring system and the synchronization-based control algorithms lack to detect zero-day attacks.

An Auxiliary Detector (AD) [14] is developed to monitor numerous sensor data discrepancies. This detector integrates observations from several sensors. However, certain deviations from the sensor readings lead to a high false rate. A rule-based isolation system is built based on the findings of all detectors to locate the source of the abnormal sensor. This method for detecting anomalies in CAN bus traffic is semantically aware during the learning phase of the system. The classifier characterizes the fields and builds a message model based on the field types. The paradigm is based on Ternary Content-Addressable Memory (TCAM) operated in either software or hardware [15]. A graph-based four-stage IDS in a CAN uses the chi-squared approach to identify severe and weak cyber threats [16]. At the same time, the IDS is inefficient when many samples are interpreted. Hence enabling safety and security for AVs and pedestrians in the IoV environment has become a primary concern. Identifying assaults in vehicular networks is crucial to prevent severe consequences due to the abnormal behavior of malicious AVs [17].

A Deep Convolutional Neural Network (DCNN)-based IDS is proposed to secure the AV's CAN bus. Further, the developed DCNN architecture is optimized for CAN bus throughput that offers a remarkable detection rate while attempting to minimize complications in the Inception-ResNet model architecture [18]. However, the model suffers from overfitting and class imbalance. IVN and EVN security attacks were analyzed and devised a multi-tiered hybrid IDS that combines a signature-based IDS with an anomaly-based IDS to categorize both threats. Every packet data transfer on an AV processor is predicted to take below 0.6 ms, indicating the feasibility of real-time incorporation of AV systems [19]. However, it fails to identify newly emerging threats and insider attacks. A data-driven anomaly detection system analyzes the pattern of CAN bus data communication. It uses real-time categorization for the early warning but lacks in learning the road behavior. To counter this, the authors investigate the link load characteristics of the IoV's Road Side Unit (RSU) in the case of various assaults resulting in irregular vehicle traffic changes [20]. Despite this, it still adds to the complexity of the network architecture. As a result, the CNN-based deep learning framework is made to extract network load characteristics that go through link load balancing's complexity and identify attacks intended at RSUs running on a testbed [21].

An anomaly-based technology that utilizes a multi-stage attention technique with a Long Short Term Memory-CNN (LSTM-CNN) architecture is proposed to detect the single and mixed multi-source anomaly. In addition, datasets are turned into vector coordinates and then examined for intrusion detection [22]. Hence, extracting the abstract features leads to higher time complexity. The usefulness of two different point models is assessed in [23] for real-time V2I attack identification using Expectation Maximization (EM) and two types of Cumulative Summation (CUSUM) algorithms (typical and adaptive). The numerical analysis demonstrates that EM, CUSUM, and adaptive CUSUM (aCUSUM) identify intrusions with minimal false positives for attacks such as DoS and impersonation. However, the system doesn't support the attacks in the V2X communication systems. A multi-stage IDS is designed to automatically discriminate against assaults while yielding a minimal number of false alerts. The suggested framework is based on a normal state-based and a DL-centered bidirectional LSTM framework that effectively detects malicious invasions from AV nodes [24]. Hence, plausibility checks must be devised for misbehavior detection rate.

Profiling of emerging attacks is necessary to withstand zero-day attacks. The study in [25] focuses on abnormal event detection and Cyber Threat Intelligence (CTI), along with massive parallelization, for the profiling and identification of developing assaults In addition to this, the position forgery attack must also be considered. A differential privacy technique is adopted in a distributed attack scenario to detect data privacy risks using distributed ML algorithms [26]. Further, a modern IDS is developed using graph-based metrics and various ML algorithms capable of combating attacks by collecting and classifying real incident data from various network vantage points [27].

The proposed IIDS framework effectively identifies the intrusions. It classifies both the in-vehicle and external vehicle threats with the safe isolation of malicious vehicles based on their severity providing a more secured IoV environment. Integrating the 5G-V2X environment enhances the transmission rate in the IoV environment leading to faster isolation of malicious AVs.

III. Vulnerabilities of Vehicular Networks

A. *Vulnerabilities of In-Vehicle Networks*

Conventional AVs consist of IVN elements and nearly 100 ECUs for facilitating numerous functionalities. CAN is responsible for communication among the ECUs in the AV system for transmitting packets, and it produces two signals, CAN-Low and CAN-High. CAN is popular because of its affordability, minimal complexity, excellent durability, noise tolerance, and fault-resistance qualities. Conversely, due to its broadcasting approach in the absence of security and unprotected prioritization mechanisms, CAN is prone to various cyberattacks [28].

The essential component of the CAN packet is the data frame, it is used to transfer AV data. A CAN packet has seven fields: the beginning of the frame, the arbitration field, the control field, the data field, the Cyclic Redundancy Code (CRC) field, the Acknowledgement (ACK) field, and the end of the frame. The data field contains 0-8 bytes, the most significant and vulnerable among all other fields. It includes the transferred data that regulates the node operations [29].

The attackers infiltrate the AVs by injecting malicious data into the CAN message packets. These message injection attacks are the most common vehicular network assaults characterized as spoofing attacks, DoS attacks, and fuzzy attacks. DoS assaults the Vehicular networks with enormous high-priority data, causing delays in legitimate interactions. Fuzzy attacks are initiated by infusing random data with arbitrarily spoofed frames, leading to rapid braking and improper gear shift adjustments in AVs. Spoofing is a form of feeding rogue packets in specific CAN identifiers that impersonate authorization and possession of the AVs; that can lead to gear spoofing and Revolutions Per Minute (RPM) spoofing in the AVs [30]. Thus, in an IoV context, IVNs are prone to generic cyberattacks, and IVNs are placed on the CAN bus line to detect and alert about these assaults.

B. *Vulnerabilities of External Vehicle Networks*

External wireless networks are used to send data between On-Board Units (OBUs) of AVs and RSUs in V2X communication. The V2X technology facilitates coordination among various IoV entities, such as AVs, infrastructures, connected devices, pedestrians, and communications networks. Dedicated Short Range Communications (DSRC), cellular networks, Remote Keyless Entry (RKE) systems, Ultra-WideBand (UWB), Radio Frequency Identification (RFID), Zigbee and Bluetooth are some of the communication networks that form the EVN. The EVN aids the AVs in localization and positioning. In addition, the EVNs are also increasing in size, including a range of different networks and systems. Intruders use vulnerabilities in the EVN systems since each AV is a possible access point for intrusions. Thus IDS is placed at the gateway of an EVN to detect and alert the intrusion.

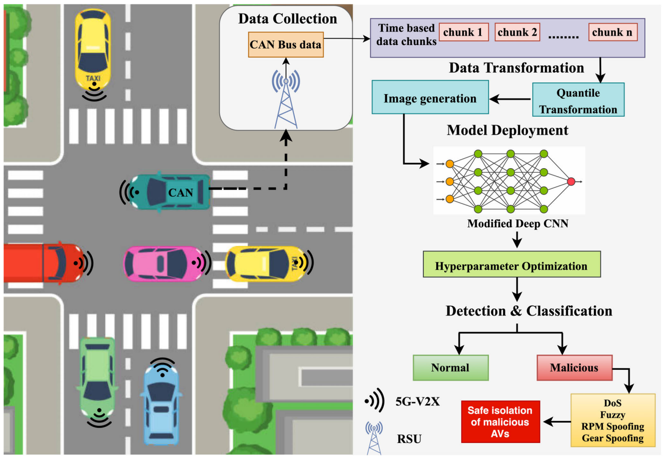


Fig. 1. Architecture diagram of the proposed IIDS framework.

IV. System Model

This section outlines the workflow of the proposed IIDS framework for providing high-end security in the IVN and EVN. The attackers launch the internal and external attacks by injecting the malicious traffic packets through On-Board Device II (OBD II) interface and other wireless interfaces. Considering the consequences of security threats on AVs, the innovative IIDS protects them from existing assaults and allows them to manage emerging threats. The modified deep CNN architecture is developed to categorize the attacks by utilizing the captured raw data from the IVN and the EVN. Normalization of data is the first step in data pre-processing and Quantile transformation is applied to obtain labels with uniform distribution. The processed data is transformed into image data for fine pattern extraction. The derived pattern-based images are trained to identify the assaults. The proposed IIDS framework utilizes hyperparameter optimization for the modified deep CNN, as shown in Fig. 1, to acquire highly accurate results. The IIDS framework is placed above the CAN network and the EVN gateways to detect the cyberattack, as shown in Fig. 2.

If an AV is found to be malicious, an alarm is triggered by the AV to notify the RSU. Concurrently the malicious AV are isolated from the EVN. Further, the RSU sends alerts to the other vehicles in the IoV ecosystem regarding malicious AVs. The proposed IIDS framework is deployed over 5G

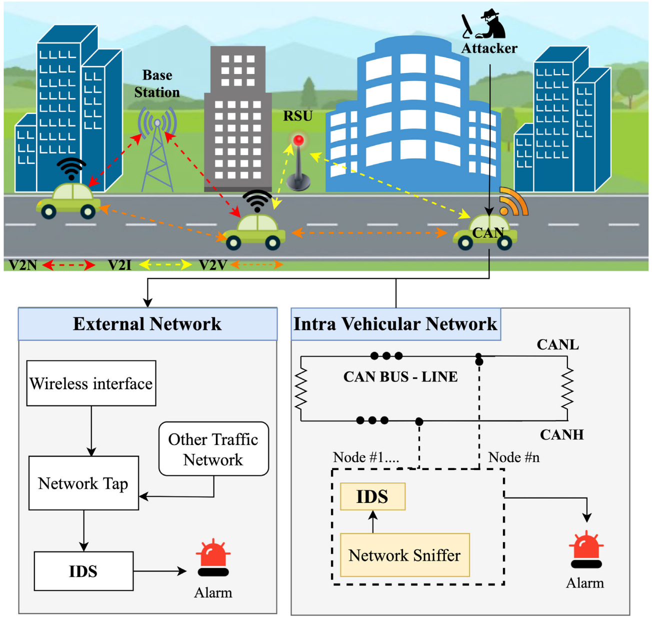


Fig. 2. Attack scenario in IVN and EVN.

networks to minimize the latency that meets the Release 15 specifications in 3GPP Releases [30], [31], [32].

V. Intelligent Intrusion Detection System

A. Traffic Model

Consider a set of AVs $(1, 2, m, \ldots, M)$ connected to at least one RSU among the RSUs $(1, 2, n, \ldots, N)$, that follows Poisson distribution in a uniform road width area. The AVs arrival rate 'X' is said to have a Poisson distribution with variance $\lambda > 0$. The Probability Density Function (PDF) given by,

$$\mathrm{F}(l; \lambda) = \Pr(X = l) = \frac{\lambda^{l} e^{-\lambda}}{l!} \tag{1}$$

where l is the number of occurrences, λ is the number of mean events in the Poisson distribution and e represents Euler number. The communication range $\aleph$ between the AV and RSU is given by,

$$\aleph_i = \nu_i \frac{\eta_i}{A_i} \tag{2}$$

Here i denote the RSUs that cover η_i AVs. The length of the road is denoted as A_i consisting of AVs with the average velocity of ν_x within i communication range. The density of vehicles that the road can occupy is highly associated with ν_i, which is given as

$$\nu_i = \max\left\{\nu_{i\,\max}\left(1 - \frac{\eta_i}{\eta_{i\,\max}}\right), \nu_{i\,\min}\right\} \tag{3}$$

$\eta_{i\,\max}$ represents the maximum number of vehicles with $\nu_{i\,\max}$, which denotes the average velocity in smooth traffic and $\nu_{i\,\min}$ is the minimum velocity of vehicles in densely populated roads with AVs.

In a free-flow traffic $\nu_{j,i}$, AV 'j' in the coverage of an RSU 'i' follows a normal distribution. Hence the PDF of $\nu_{j,i}$ is given by,

$$F\left(\nu_{j,i}\right) = \frac{1}{\sqrt{2\pi}\phi} e^{-\frac{(\nu_{j,i} - \nu_i)^2}{2\phi^2}} \tag{4}$$

To avoid the negative truncated value of $\nu_{j,i}$, it is further illustrated as

$$\widehat{F\left(\nu_{j,i}\right)} = \frac{\mathrm{F}\left(\nu_{j,i}\right)}{\int_{\nu_{i\,\min}}^{\nu_{i\,\max}} \mathrm{F}\left(\nu_{j,x}\right) d\nu_{j,i}} \tag{5}$$

$$\widehat{F\left(\nu_{j,i}\right)} = \frac{2\,\mathrm{F}\left(\nu_{j,i}\right)}{\Psi\left(\frac{\nu_{i\,\max} - \bar{\nu}_i}{\sqrt{2}\phi}\right) - \Psi\left(\frac{\nu_{i\mathrm{min}} - \bar{\nu}_i}{\sqrt{2}\phi}\right)} \tag{6}$$

where $\Psi(G)$ is the Gauss error function and it can be denoted by

$$\Psi(G) = \sqrt{\frac{2}{\pi}} \int_0^G e^{-\eta^2} d\eta \tag{7}$$

where the integral values range from 0 to the error G.

B. Threat Model

The IVN is affected by injecting malicious CAN messages or restricting the vital messages from being sent. It affects the AV's connectivity and motor control as most onboard components are vulnerable to attacks. IDS is highly essential to monitor malicious activities to secure AVs. For example, GPS spoofing and DoS are two of the most significant threats to AV components.

GPS spoofing causes denial of location sharing and sometimes provides false location information to AVs. DoS prevents the timely transmission of messages in AVs. These attacks threaten the normal functioning of the IoV ecosystem; hence the IDS is placed above the CAN in IVN. As the messages from CAN to the other nodes are broadcasted, the messages must pass through IDS for scanning. Whenever the IDS detects an attack, changes in the CAN signals will lead to alarm initiation to alert the nodes.

Meanwhile, the EVN can also be intruded upon with malicious messages that create chaos among the AVs to coordinate in the IoV system. External network attacks collapse the entire IoV system and lead to abnormal traffic. The attackers may inject false information along with the packets sent between AVs to create chaos in the traffic. The IDS helps prevent intrusions; thus, AVs can communicate with the IoV system after analyzing the packets through IDS. Whenever the IDS detects an attack in the external networks, an alarm will be triggered, and the attacker's access will be revoked immediately. Thus the data breach can be avoided in both IVN and EVN, as depicted in Fig.2.

C. Modified Convolutional Neural Network

The modified CNN comprises numerous layers of artificial neurons that compute the weighted sum of multiple inputs, outputs, and activation values. An equation calculates the final output φ of an artificial neuron b with input ϱ that includes AV

Identifier (ID), total AVs in the IoV environment, AV generated data ß, the vehicular dynamics data $\wp$ along with threshold limit £ for better intrusion detection. φ is represented as

$$\varphi^{(b)} = \mathcal{F}\left(\varrho^{(b-1)} * \delta^{(b-1)} + \beta^{(b-1)}\right) \tag{8}$$

δ corresponds to a vector representing the weight, and β denotes the bias. Numerous data are given to input nodes in CNN, and each input is assigned a weight. The incline of the activation function tends to increase with weight, and the bias determines the latency caused to trigger the activation function. Considering the inputs $\varrho1$, $\varrho2$, and $\varrho3$ given to a typical neuron with synaptic weights $\delta1$, $\delta2$, and $\delta3$, the output function τ is calculated as

$$\tau = \mathcal{F}(\varrho) = \Sigma \varrho_x \delta_x; \quad x \geq 1 \tag{9}$$

The activation function in the CNN has various choices. We consider the sigmoid activation function, also known as the logistic activation function, non-linear. The sigmoid activation function $\mathcal{S}$ is derived from $\mathcal{F}'(\varrho)$.

$$\mathcal{F}(\varrho) = \frac{1}{1+e^{-\varrho}} \tag{10}$$

where $\mathcal{F}(\varrho)$ is differentiable and provides a smooth gradient. Thus the derivative of $\mathcal{F}'(\varrho)$ with '$\mathcal{S}$' is computed as

$$\mathcal{F}'(\varrho) = \mathcal{S}(\varrho)^*(1-\mathcal{S}(\varrho)) \tag{11}$$

Several sigmoid activations are employed at the final layer of the deep layers to learn a unique distribution for multi-label classification. The training updates a set of weights and biases that will allow the model to integrate the input-output correlation.

Backpropagation is one of the most prevalent training approaches where w is adjusted to minimize the actual and predicted output vector variance. It also aims to reduce the cost function that estimates the re-balancing level with weight, bias, and activation function. The training sample loss $\left(\varrho^{(p)}, \tau^{(p)}\right)$ is illustrated as,

$$\Omega\left(\delta, \beta, \varrho^{(p)}, \tau^{(p)}\right) = \frac{1}{2}\left\| h_{\delta,\beta}\left(\varrho^{(p)}\right) - \tau^{(p)}\right\|^2 \tag{12}$$

$h(\delta, \beta)(\varrho^{(p)})$ denotes the output of the trained neural network. Hence the loss function for M training samples can be derived as,

$$\Omega(\delta, \beta) = \frac{1}{p}\sum_{p=1}^{P} \Omega\left(\delta, \beta, \varrho^{(p)}, \tau^{(p)}\right) \tag{13}$$

Backpropagation utilizes gradient descent to find the optimal result by reducing the loss function. The partial derivatives of gradient descent $\partial\Omega\partial\delta^{(b)}_{x,y}$ and $\partial\Omega\partial\beta^{(b)}_{x,y}$ and ∂B are computed using the error term of backpropagation. The weight $\delta^{(b)}_{x,y}$ is connected with the neuron y in b^{th} layer and neuron x in the $b+1^{th}$ layer. $\beta(l)$ represents the bias in neuron x in the $\Omega + 1^{th}$ layer. The variables are associated as,

$$\begin{cases} \delta^{(b)}_{x,y} = \delta^{(b)}_{x,y} - \rho\dfrac{\alpha\Omega}{\alpha\delta^{(b)}_{x,y}} \\ \beta^{(b)}_{x} = \beta^{(b)}_{x} - \rho\dfrac{\alpha\Omega}{\beta^{(b)}_{x}} \end{cases} \tag{14}$$

Algorithm 1 IIDS for Attack Detection, Classification & Isolation of Malicious Vehicles

Input: AV ID, Total AVs, AV data ß, AV dynamics data $\wp$, threshold limit £

Output: Attack classification, Deviation ϖ, loss ø, and accuracy Å

```
for time epoch do
    for $i = 1$ to $n$ in $AV_i$ do
        if $\wp$ != empty then
            Initialize numpy array
            Perform ß transformation
            Sample the batch of data from training set
            Calculate loss function according to (11)
            Calculate $\partial\Omega\partial\delta^{(l)}_{i,j}$ and $\partial\Omega\partial\beta^{(l)}_{i,j}$
            Update the parameters of layer based on $\partial\Omega\partial\delta^{(l)}_{i,j}$
            and $\partial\Omega\partial\beta^{(l)}_{i,j}$ according to (13)
            Process backpropagation according to (15)
            Return ø, Å, $\varpi$, attack classification
        end if
        for attack classification = true do
            Determine Threshold limit £
            Calculate and update $\varpi$
            Update the variance
        end for
        for $i = 1$ to $n$ in $AV_i$ do
            if attack classification >= £
             then
                Isolate AV from network
                Halt AV
            end if
            if attack classification <= £
             then
                Restore driving functionality
                Restore VANET integration
                Continue functionality
            end if
            Update AV condition
        end for
    end for
end for
```

α represents the learning rate of the deep CNN. The error term e is determined by the difference of the training sample $y^{(p)}$ with the matching result trace $h_{(\delta,\beta)}(\varrho^{(p)})$ to acquire these partial derivatives. e for any neuron in the output layer is formulated as follows,

$$e^{(n\Omega)}_x = -\left(\tau_x - \varphi x^{(n\Omega)}\right) \times \mathcal{F}'\left(z^{(n\Omega)}_x\right) \tag{15}$$

n_x denotes the total number of layers. Thus the backpropagation occurring in the CNN is given by

$$e^{(\Omega)}_x = \left(e^{(b+1)}_x \bigotimes 1_{Q\times Q}\right) \circ \mathcal{F}'\left(z^{(\Omega)}_x\right) \tag{16}$$

where '$\bigotimes$' and '$*$' denote the Hadamard product and the Kronecker product, respectively. The pooling layer accompanied by a convolutional layer is represented as

$$e_x^{(\Omega)} = \left(e_x^{(\Omega+1)} * r\left(\delta_x^{(\Omega+1)}\right)\right) \circ \mathcal{F}'\left(z_x^{(\Omega)}\right) \tag{17}$$

The function r represents a 180 degree rotational matrix. After rotation, the partial derivatives are computed as

$$\begin{cases} \dfrac{\partial \Omega}{\partial \delta_{x,y}^{(b)}} = \sum_{u,v} \left(e_x^{(\Omega)}\right)_{u,v} \left(\varphi_y^{(\Omega-1)}\right)_{u,v} \\ \dfrac{\partial B}{\partial \beta_x^{(b)}} = \sum_{u,v} \left(e_x^{(\Omega)}\right)_{u,v} \end{cases} \tag{18}$$

where $\left(\varphi_y^{(\Omega-1)}\right)_{u,v}$ is the element at (u, v) in the result map of the $b - 1^{th}$ layer.

D. Modified Deep Architecture of IIDS

The deep architecture of IIDS is designed for intrusion detection that comprises 13 layers with seven convolution layers, three pooling layers, two dense layers, and one dropout layer. Two layers belong to max-pooling in the pooling layer, and one belongs to the global average pooling. The link load data of an AV is represented as θ, where $\theta = [\theta_1, \theta_2, \ldots, \theta_n]$. For a training sample (θ, c), c is the output map that determines whether the network is intruded or not. The c of the initial convolutional layer is calculated as,

$$\xi_y^{(2)} = \mathcal{S}\left(\theta * \varrho_y^{(1)} + \omega_y^{(1)}\right), \quad y \in \Theta^{(1)} \tag{19}$$

The collection of kernels in the initial convolution layer is represented by $\Theta^{(1)}$.The traffic flow in an IoV exhibit more erratic variations than in other networks like IP backbone network. Along with this aggregated traffic flow, the link node loads in AVs also produce dynamic fluctuations, which is the central issue of malware detection in IoV. We employ average pooling to obtain irregular swings and other spatial properties, which may be expressed as follows

$$\xi_y^{(3)} = \mathcal{A}\left(\xi_y^{(2)}\right), \quad y \in \Theta^{(2)} \tag{20}$$

Here ξ_y denotes a subset of input maps in the initial pooling layer, and $\mathcal{A}$ denotes average pooling. Similarly, the propagation of pooling and convolutional layers are depicted by

$$\begin{cases} \xi_y^{(4)} = \mathcal{S}\left(\sum_{y \in a^{(2)}} \xi_x^{(3)} * \varrho_{x,y}^{(3)} + \omega_y^{(3)}\right), & y \in \Theta^{(3)} \\ \xi_y^{(5)} = \mathcal{A}\left(\xi_y^{(4)}\right), & y \in \Theta^{(4)} \\ \xi_y^{(6)} = \mathcal{S}\left(\sum_{x \in a^{(3)}} \xi_x^{(5)} * \varrho_{x,y}^{(5)} + \omega_y^{(5)}\right), & y \in \Theta^{(5)} \\ \xi_y^{(7)} = \mathcal{A}\left(\xi_y^{(6)}\right), & y \in \Theta^{(6)} \end{cases} \tag{21}$$

where a is the output maps of the layer b. A fully interconnected layer is introduced before the output layer, with the sigmoid function as the activation function. Further, the output map is represented as follows,

$$h_{\phi,\omega}(\boldsymbol{\theta}) = \mathcal{S}\left(\sum_{x \in a^{(2)}} \xi_x^{(7)} * \phi_{x,y}^{(7)} + \omega_y^{(7)}\right), \quad y \in \Theta^{(7)} \tag{22}$$

To train the deep architecture, backpropagation is presented to adjust the parameters, including kernels and bias. During the training phase, we consider a loss function that relies on the first form of normalization, defined as

$$\mathcal{B}(\phi, \omega, \theta, c) = \frac{1}{2}\left\|h_{\phi,\omega}(\theta) - c\right\|^2 \tag{23}$$

On considering γ samples, the loss function is devised as

$$\mathcal{B}(\phi, \omega) = \frac{1}{\gamma}\sum_{p=1}^{\gamma} \mathcal{B}\left(\phi, \omega, \boldsymbol{\theta}^{(p)}, c^{(m)}\right) \tag{24}$$

A redundant error term is used to improve the training error's convergence and to reduce the loss and backpropagation error. Thus loss function after the addition of redundant error term is calculated by,

$$\begin{cases} \hat{\mathcal{B}}(\phi, \omega) = \mathcal{B}(\phi, \omega) + \tilde{\mathcal{B}}(\phi, \omega) \\ \mathcal{B}(\phi, \omega) = \dfrac{1}{2\gamma}\sum_{p=1}^{\gamma} \left\|h_{\phi,\omega}\left(\theta^{(p)}\right) - c^{(p)}\right\|^2 \\ \tilde{\mathcal{B}}(\phi, \omega) = \dfrac{1}{2\gamma}\sum_{p=1}^{\gamma} \left\|h_{\phi,\omega}\left(\theta^{(p)}\right) - \tilde{y}^{(p)}\right\|^2 \end{cases} \tag{25}$$

where $\tilde{\mathcal{B}}$ is denoted as the redundant loss. The error term of the output layer is computed as

$$\varepsilon_x^{(8)} = -\left(c_x - \xi_x^{(8)}\right) \times f'\left(a_x^{(8)}\right), \quad x = \{1, 2, 3\} \tag{26}$$

$$\varepsilon_x^{(7)} = \left(\sum_{y=1}^{\Theta^{(8)}} \phi_{yx}^{(7)} \varepsilon_y^{(8)}\right) f'\left(a_x^{(7)}\right) \tag{27}$$

$\varepsilon_3^{(8)}$ is the redundant error term and in case of fully connected layer, the error term is denoted by

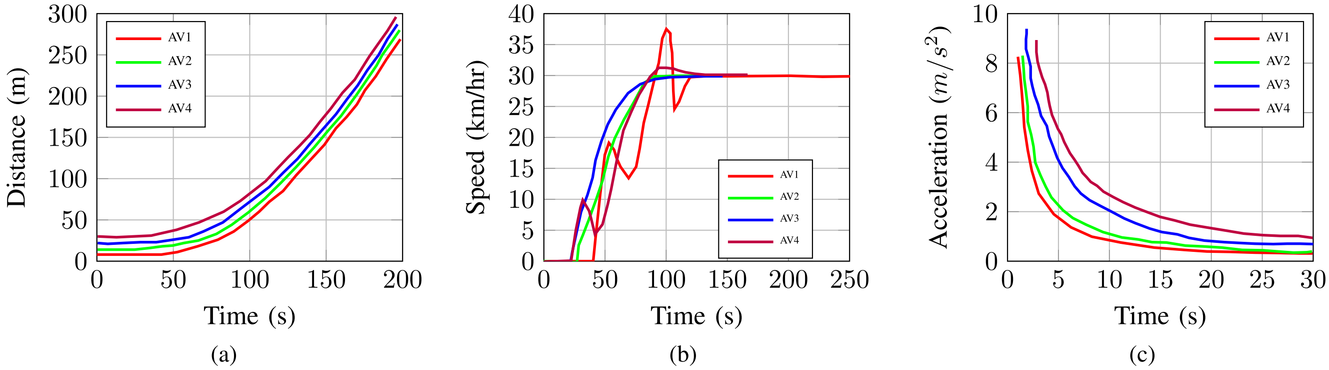
$$\Delta\varepsilon_x^{(7)} = \phi_{3x}^{(7)} \varepsilon_3^{(8)} f'\left(a_x^{(7)}\right), \quad x = \left\{\Theta^{(7)}\right\} \tag{28}$$

Thus, the redundant error term enhances the convergence of the error during the model's training phase. Finally, the validation of the model and accuracy are devised for the classification label. The modified CNN is subjected to hyperparameter optimization to provide better results and choose the optimal parameters.

E. Hyperparameter Optimization

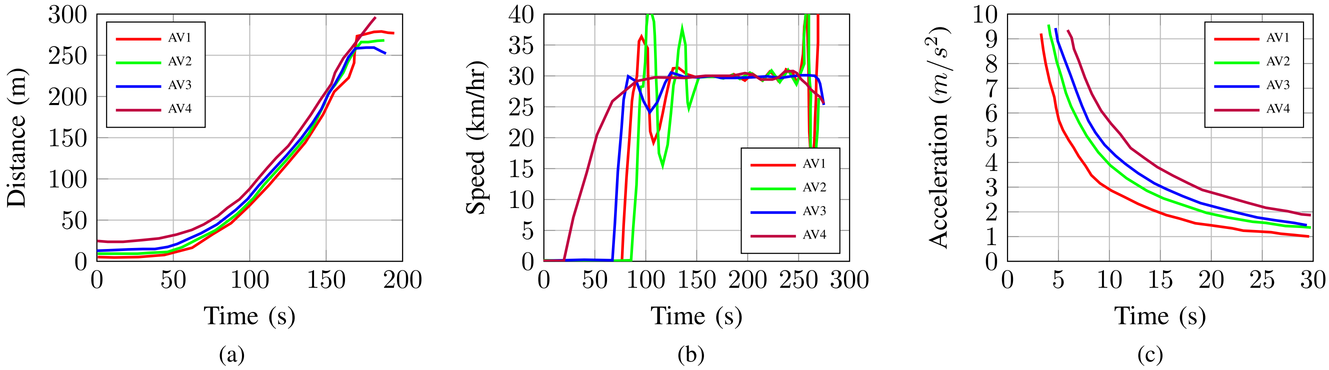
Deep CNN models have several hyperparameters that must be tuned. Model-training and model-design hyperparameters are the two types of hyperparameters. The fraction of freeze layers, dropout rate, and learning rate are model-design hyperparameters that are established throughout the model design process in the proposed IIDS framework. To optimize the training time and model performance, model-training hyperparameters are utilized in the IIDS by adjusting sample size, epoch count, and early stop. These hyperparameters influence the modified CNN model's structure, reliability, and overall performance.

In Algorithm V-C, the total AVs of the IoV environment, their unique IDs, AV dynamics data, AV data and threshold limit are given as the input. The proposed IIDS performs data transformation followed by attack detection and classification. Further, the deviation, loss, and accuracy are obtained to determine the isolation of AVs as an output.



(a) (b) (c)

Fig. 3. Motion analysis of AVs: before attack scenario (a) Distance (b) Speed (c) Acceleration.



(a) (b) (c)

Fig. 4. Motion analysis of AVs: after attack scenario (a) Distance (b) Speed (c) Acceleration.

VI. Performance Evaluation

A. Experimental Setup

The IIDS framework is evaluated by simulating the IoV scenario on the Network Simulator-2 (NS2). The mobility scenario of AVs is generated using Simulation of Urban Mobility (SUMO). The simulation is carried out for around 3000 seconds to monitor the parameters. The data transmission using a 5G network is configured at 3.5 GHz, relying on the 3GPP Release 15.

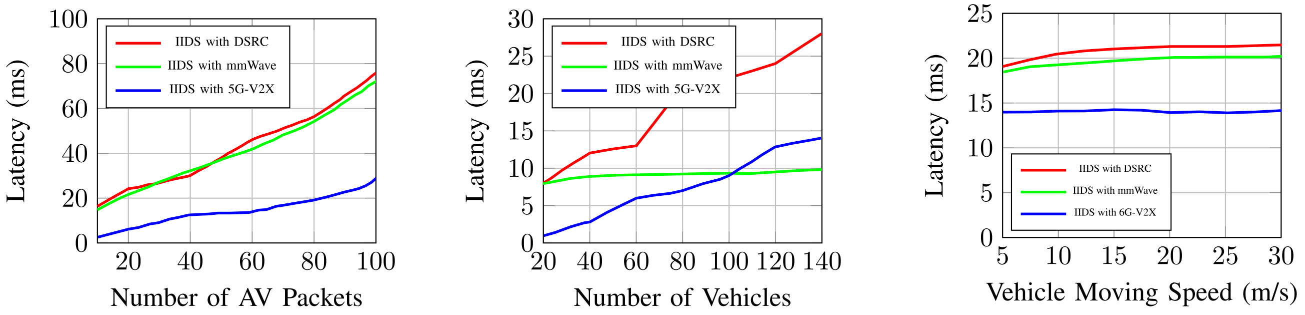
B. Analysis of Distance, Speed and Acceleration Error Rate

The IVN comprises the data acquired from the OBUs via the CAN bus. The vehicular dynamics parameter's data determine the AVs driving style in the IoV platform. Apart from broadcasting these vehicular dynamics data, monitoring the deviation in the parameters is essential to detect the level of AV misbehavior.

Balancing speed, distance, and acceleration are essential to maintain smooth traffic and achieve hassle-free autonomous driving in the IoV environment. It also helps improve AVs' detection accuracy and malicious level. The vehicular dynamics data of 4 AVs are taken into consideration. Fig. 3 depicts AV's position, speed, and acceleration before an attack happens, and Fig. 4 represents the motion of AVs after the attack. All AVs travel without movement distortion without an attack, as depicted in Fig. 3(a). As a result, AVs' speed and acceleration are not divergent, as demonstrated in Fig. 3(b) and Fig. 3(c). However, as shown in Fig. 4(a), the AVs that are exposed to assaults that incur high deviation, the distance traveled to reach the destination also shows a huge increase. Due to the malicious nature of AVs, there are sudden fluctuations in their speed and acceleration, which causes chaos in the traffic, as illustrated in Fig. 4(b) and Fig. 4(c).

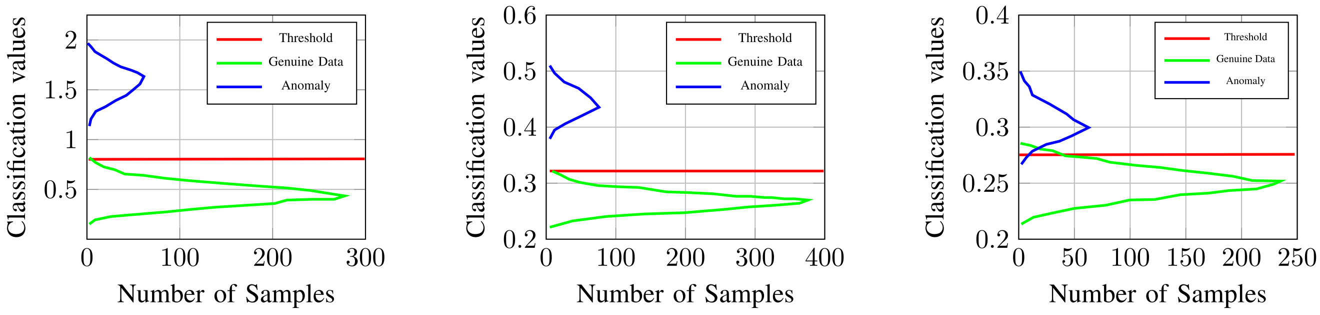
C. Analysis of Latency

Fig. 5(a) compares the delay in message transmission for the various scenarios in the proposed IIDS with the DSRC and millimeterWave (mmWave) communications. A detailed examination of the plots indicates that the proximity between 5G-V2X and the other VANETs (DSRC, mmWave) is more prominent in the top-performing IIDS framework. As a result, the suggested IIDS framework performs efficiently when combined with 5G-V2X, as it provides more bandwidth. Fig. 5(b) depicts the average message transmission delay occurring with the number of vehicles in the IoV environment. According to the plot, 5G-V2X can handle more AVs in the IoV environment than the other networking technologies. The average message delay is plotted in Fig. 5(c) based on the AV moving speed. Propagation delay is ubiquitous in all networking technologies. Hence, it is unpredictable in the case of dynamic sender and receiver. AVs suffer a lot of distortion as they move quickly over a distance at a specific time. The graph shows that 5G-V2X outperforms the DSRC and mmWave, having the lowest message delay in the dynamic IoV environment.



(a) (b) (c)

Fig. 5. Latency analysis (a) Packet transmission delay (b) Message transmission delay with total vehicles (c) Message transmission delay with vehicle moving speed.



(a) (b) (c)

Fig. 6. Analysis of attack scenarios (a) DoS attack (b) Fuzzy attack (c) Spoofing attack.

D. Analysis of Attack Scenarios

1) Analysis of DoS Attack Scenario: The cyber attacker attempts to interrupt ECU connectivity in a DoS attack by overloading the CAN bus with high-priority packets. Consequently, the bus becomes congested with arbitrary CAN messages, and several important messages are either deferred or never sent. Fig. 6(a) highlights the effectiveness of the proposed IIDS under evaluation in the DoS condition compared to the optimal threshold classification values.

2) Analysis of Fuzzy Attack Scenario: In a fuzzy attack, the intruder need not be familiar with CAN packets. By transmitting a pseudorandom sequence of ID, data size, and the number of bits, the remote hacker can assault the system that causes the AVs to break down. It includes irregular gear shifts, a shaky steering wheel, etc. Fig. 6(b) displays the model performance for the scenario under fuzzy attack consideration. As the determined optimal threshold results, the proposed IIDS outperforms all models in this circumstance.

3) Analysis of Spoofing Attack Scenario: The hacker introduces false packets by profiling specific CAN IDs. The injected malicious packets target the CAN ID in spoofing. Spoofing makes it impossible for ECUs to differentiate genuine messages from injected messages, leading the AVs to collapse. The two types of spoofing attacks considered are the Gear and RPM spoofing attacks. The effectiveness of different models for these assaults is depicted in Fig. 6(c). Once again, the proposed IIDS performs more efficiently than any other existing model.

E. Performance Analysis of IIDS Framework

The IIDS predicts the proper attack type by labeling the test data based on the potential attacks. The successful deployment of the model depends upon the high number of correct label classifications based on true and false positives. The proposed IIDS is evaluated based on precision, recall, F1-score, True Positive Rate (TPR), False Positive Rate (FPR), and false alarm rate. A true positive rate is an outcome where the system correctly predicts the potential attacks. Similarly, a false positive rate is an outcome where the model incorrectly predicts the potential attacks. False alarm rate is the probability of falsely rejecting the null hypothesis for a particular test case. As discussed in Section II, IIDS is compared with state-of-art models, namely, Auxiliary Detector (AD), Convolutional Neural Networks (CNN), Long Short Term Memory-Convolutional Neural Network (LSTM-CNN), Deep Convolutional Neural Network (DCNN) and the detailed analysis are further illustrated in Fig. 7 and Fig. 8.

1) Precision: Precision is a metric for determining the amount to which true positives are correct. Precision has increased by 1-2% for most classifiers. The SVM method shows the greatest improvement over other algorithms. The SVM method shows the greatest improvement over other algorithms. However, the IIDS framework outperforms all other models.

2) Recall: The percentage of effective identification of malicious occurrences is represented by the True Positive Rate (TPR), also known as recall. When analyzing the findings of studies in terms of TPR, the results are very comparable

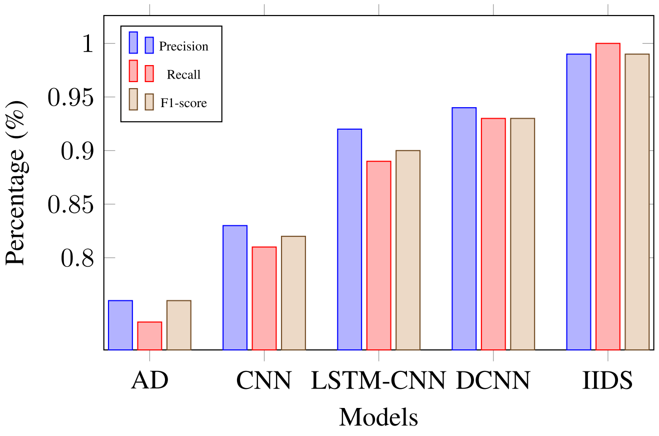


Fig. 7. Performance analysis of the proposed IIDS framework with various algorithms.

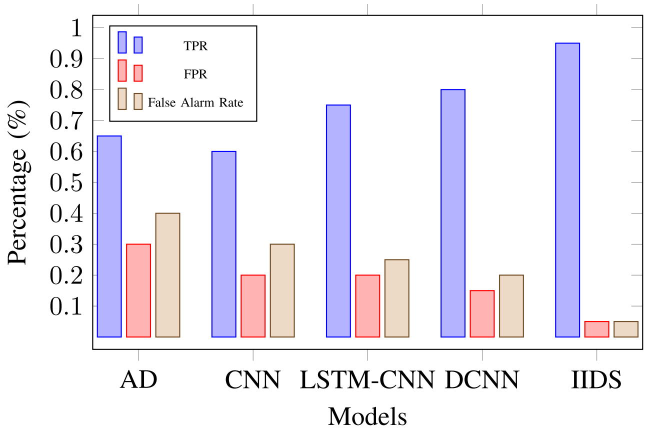


Fig. 8. Comparitive study of the proposed IIDS framework with other exisiting systems.

to those of precision. DT tends to have a higher recall rate following the proposed IIDS mechanism.

3) F1-Score: The F1-score measures a test's accuracy, often known as the F-measure. It is computed using precision and recall by equaling the number of true positive results divided by the total number of positive results. It includes results that are incorrectly identified and then recalled by equaling the number of true positive results divided by the total number of samples identified as positive. IIDS achieves the highest F1 score from the analysis, followed by DT and SVM. Thus the proposed system is efficient in detecting and classifying cyberattacks.

Furthermore, TPR, FPR and false alarm rates are compared and analyzed with the other existing systems. From Fig. 7, it is clear that the proposed IIDS system incurs less FPR and false alarm rate and tends to be efficient in generating real alert alarms.

VII. Conclusion & Future Works

AVs are susceptible to cyberattacks due to the lack of authentication and salient security mechanisms in the widely used IVN and EVN. This paper proposes a novel IIDS framework for efficient intrusion detection and classification of cyberattacks using modified deep CNN architecture with hyperparameter optimization. On the other hand, AVs are isolated when they are found to be malicious. The adopted deep architecture technique enhances the decision-making strategy for intrusion detection and classification in the 5G-V2X environment. The experimental results depict that the IIDS system outperforms the existing models by achieving 98% accuracy with high reliability. Future works can look towards the various methods of re-integrating the malicious AVs into the network once it is normal. Zero-day attack detection and mitigation strategies can be examined based on the attack patterns.

References

[1] S. Liu, Y. Yu, W. Hu, Y. Peng, and X. Yang, "Intelligent vulnerability analysis for connectivity and critical-area integrity in IoV," *IEEE Access*, vol. 8, pp. 114239–114248, 2020.

[2] G. Raja, P. Dhanasekaran, S. Anbalagan, A. Ganapathisubramaniyan, and A. K. Bashir, "SDN-enabled traffic alert system for IoV in smart cities," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 1093–1098.

[3] J. Zhou et al., "A model-based method for enabling source mapping and intrusion detection on proprietary can bus," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 3, 2022, doi: 10.1109/TITS.2022.3153718.

[4] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola, and A. Benslimane, "NovelADS: A novel anomaly detection system for intra-vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 22596–22606, Feb. 2022, doi: 10.1109/TITS.2022.3146024.

[5] H. Zhong, W. Cao, Q. Zhang, J. Zhang, and J. Cui, "Toward trusted and secure communication among multiple internal modules in CAV," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17734–17746, Dec. 2021.

[6] G. Raja, S. Anbalagan, S. Senthilkumar, K. Dev, and N. M. F. Qureshi, "SPAS: Smart pothole-avoidance strategy for autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 1–10, Apr. 2022.

[7] L. Von Rueden et al., "Informed machine learning—A taxonomy and survey of integrating prior knowledge into learning systems," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 1, pp. 614–633, Jan. 2021, doi: 10.1109/TKDE.2021.3079836.

[8] B. Dhanalaxmi, "Machine learning and its emergence in the modern world and its contribution to artificial intelligence," in *Proc. Int. Conf. Emerg. Technol. (INCET)*, Jun. 2020, pp. 1–4.

[9] S. B. Prathiba, G. Raja, S. Anbalagan, S. Gurumoorthy, N. Kumar, and M. Guizani, "Cybertwin-driven federated learning based personalized service provision for 6G-V2X," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4632–4641, May 2022.

[10] S. V. Balkus, H. Wang, B. D. Cornet, C. Mahabal, H. Ngo, and H. Fang, "A survey of collaborative machine learning using 5G vehicular communications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1280–1303, 2nd Quart., 2022.

[11] G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M. Baskaran, K. Raja, and A. K. Bashir, "Intelligent reward-based data offloading in next-generation vehicular networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3747–3758, May 2020.

[12] A. Petrillo, A. Pescapé, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134–1149, Mar. 2021.

[13] X. Han et al., "ADS-Lead: Lifelong anomaly detection in autonomous driving systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 1–13, Jan. 2022.

[14] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, "Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8247–8259, Jul. 2022, doi: 10.1109/TITS.2021.3077015.

[15] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Veh. Commun.*, vol. 9, pp. 43–52, Jul. 2017.

[16] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2122–2134, Feb. 2023, doi: 10.1109/TITS.2021.3128634.

[17] M. Cui, J. Wang, and M. Yue, "Machine learning-based anomaly detection for load forecasting under cyberattacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5724–5734, Sep. 2019.

[18] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 14–25, 2021.

[19] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for Internet of Vehicles," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1397–1409, Jul. 2021.

[20] M. Li, F. R. Yu, P. Si, W. Wu, and Y. Zhang, "Resource optimization for delay-tolerant data in blockchain-enabled IoT with edge computing: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9399–9412, Oct. 2020.

[21] W. Serrano, "The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102909.

[22] L. Shi, X. Li, Z. Gao, P. Duan, N. Liu, and H. Chen, "Worm computing: A blockchain-based resource sharing and cybersecurity framework," *J. Netw. Comput. Appl.*, vol. 185, Jul. 2021, Art. no. 103081, doi: 10.1016/j.jnca.2021.103081.

[23] R. Mills, A. K. Marnerides, M. Broadbent, and N. Race, "Practical intrusion detection of emerging threats," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 582–600, Mar. 2022, doi: 10.1109/TNSM.2021.3091517.

[24] P. Ramanan, D. Li, and N. Gebraeel, "Blockchain-based decentralized replay attack detection for large-scale power systems," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 8, pp. 4727–4739, Aug. 2022, doi: 10.1109/TSMC.2021.3104087.

[25] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1189–1201, Apr. 2021.

[26] G. Raja, S. Anbalagan, G. Vijayaraghavan, S. Theerthagiri, S. V. Suryanarayan, and X. Wu, "SP-CIDS: Secure and private collaborative IDS for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4385–4393, Jul. 2021.

[27] H. Sadreazami, A. Mohammadi, A. Asif, and K. N. Plataniotis, "Distributed-graph-based statistical approach for intrusion detection in cyber-physical systems," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 137–147, Mar. 2018.

[28] Y. Lin, C. Chen, F. Xiao, O. Avatefipour, K. Alsubhi, and A. Yunianta, "An evolutionary deep learning anomaly detection framework for in-vehicle networks—CAN bus," *IEEE Trans. Ind. Appl.*, early access, Jul. 17, 2020, doi: 10.1109/TIA.2020.3009906.

[29] Y. Xun, J. Liu, and Y. Zhang, "Side-channel analysis for intelligent and connected vehicle security: A new perspective," *IEEE Netw.*, vol. 34, no. 2, pp. 150–157, Mar. 2020.

[30] Y. Xun, Y. Zhao, and J. Liu, "VehicleEIDS: A novel external intrusion detection system based on vehicle voltage signals," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2124–2133, Feb. 2022.

[31] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019.

[32] A. Hoglund, D. P. Van, T. Tirronen, O. Liberg, Y. Sui, and E. A. Yavuz, "3GPP release 15 early data transmission," *IEEE Commun. Standards Mag.*, vol. 2, no. 2, pp. 90–96, Jun. 2018.