Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Security strategy for autonomous vehicle cyber-physical systems using transfer learning

Abdulaziz A. Alsulami[1], Qasem Abu Al-Haija[2*], Badraddin Alturki[3], Ali Alqahtani[4] and Raed Alsini[1]

Abstract

Cyber-physical systems (CPSs) are emergent systems that enable effective real-time communication and collaboration (C&C) of physical components such as control systems, sensors, actuators, and the surrounding environment through a cyber communication infrastructure. As such, autonomous vehicles (AVs) are one of the fields that have significantly adopted the CPS approach to improving people's lives in smart cities by reducing energy consumption and air pollution. Therefore, autonomous vehicle-cyber physical systems (AV-CPSs) have attracted enormous investments from major corporations and are projected to be widely used. However, AV-CPS is vulnerable to cyber and physical threat vectors due to the deep integration of information technology (IT), including cloud computing, with the communication process. Cloud computing is critical in providing the scalable infrastructure required for real-time data processing, storage, and analysis in AV-CPS, allowing these systems to work seamlessly in smart cities. CPS components such as sensors and control systems through network infrastructure are particularly vulnerable to cyber-attacks targeted by attackers using the communication system. This paper proposes an intelligent intrusion detection system (IIDS) for AV-CPS using transfer learning to identify cyberattacks launched against connected physical components of AVs through a network infrastructure. First, AV-CPS was developed by implementing the controller area network (CAN) and integrating it into the AV simulation model. Second, the dataset was generated from the AV-CPS. The collected dataset was then preprocessed to be trained and tested via pre-trained CNNs. Third, eight pre-trained networks were implemented, namely, InceptionV3, ResNet-50, ShuffleNet, MobileNetV2, GoogLeNet, ResNet-18, SqueezeNet, and AlexNet. The performance of the implemented models was evaluated. According to the experimental evaluation results, GoogLeNet outperformed all other pre-rained networks, scoring an F1- score of 99.47%.

Keywords Cyber-physical system (CPS), Cyber security (CSec), Intrusion detection system (IDS), Autonomous vehicle (AV), Deep learning (DL), Transfer learning (TL), Controller area network (CAN)

Introduction

Autonomous Vehicles (AVs) have recently been developing rapidly, and some smart or self-driving cars can be found on public roads [1]. Furthermore, AVs have been a trending topic in academia and business as many people have started understanding the unlimited benefits of this technology [2]. AVs can execute sophisticated tasks like lane departure warnings, traffic sign identification, and avoiding collisions, and they can also reduce the workload of human drivers [3]. Furthermore, the operation of AVs positively impacts the environment by reducing energy consumption and air pollution [4]. AVs typically have sophisticated computing, sensing, and

*Correspondence:
Qasem Abu Al-Haija
qsabuhaija@just.edu.jo
[1] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, 21589 Jeddah, Saudi Arabia
[2] Department of Cybersecurity, Faculty of Computer & Information Technology, Jordan University of Science and Technology, PO Box 3030, Irbid 22110, Jordan
[3] Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, 21589 Jeddah, Saudi Arabia
[4] Department of Networks and Communications Engineering, College of Computer Science and Information Systems, Najran University, 61441 Najran, Saudi Arabia

actuating systems based on heterogeneous architectural designs. However, numerous inherent difficulties exist with networking and communication technologies, including security, privacy, data transmission, real-time data analytics, and bandwidth restrictions [5]. In response to technological advancements in smart transportation systems, AVs may transmit data via various communication protocols. A cyber-physical system (CPS) is a system that uses contemporary sensor, computation, and network technology to merge cyber and physical components seamlessly [6]. AV provides the perfect fit model of a CPS when integrated with electronic and physical equipment [7]. Several vehicle network systems, like sensors, actuators, and electronic control units (ECUs), can connect AV components. The most popular network systems are controller area networks (CAN), Time-Triggered CAN (TTCAN), Local Interconnect Networks (LIN), and FlexRay [8]. CAN protocol was invented by Bosch researchers in 1985 to replace the wires in the automotive system because the number of wires started to increase, resulting in a degradation in reliability [9]. CAN is a standard communications protocol that can be used for vehicle control sensor data [10]. However, the CAN can process a small number of real-time sensor data [10].

Additionally, the data flow from numerous automotive core control systems, including the engine, transmission system, body system, and other electrical equipment, is collected via the CAN bus, and every bit of information is broadcast to the CAN bus. Every node has perpetual access to the network, which states that harmful internal or external information might attack any CAN network node in a vehicle [11]. Understandably, the AVs must be equipped with more sensing and communication equipment to function independently. Figure 1 shows essential AV components. However, when the degree of autonomy increases, so do the security dangers [12]. Attack sources are often negative internal components or external events intended to undermine the AV's expected autonomy [11]. The attack surfaces of AVs can be Airbag ECU, USB, Bluetooth, Vehicle access system ECU, etc., as identified in [13].

In the context of smart cities, AVs are a key application of CPS principles, helping to improve urban living by decreasing energy consumption and minimizing air pollution. Integrating information technology (IT) and communication processes in AV-CPS, including cloud computing, is crucial in providing the scalable infrastructure required for real-time data processing, storage, and analysis in AV-CPS, allowing these systems to operate

Fig. 1 Autonomous vehicle architecture

seamlessly in smart cities. Furthermore, AVs are susceptible to cyberattacks such as key fob cloning attacks, radar attacks, telematics service attacks, sensors spoofing attacks, ultrasonic sensor attacks, lidar sensor attacks, camera sensor attacks, and others, also new risks like ransomware and vehicle theft [14]. Therefore, this paper proposes a method based on a pre-trained convolutional neural network (CNN), which helps to detect cyberattacks conducted through the CAN communication protocol to target the connected physical components of AVs. With the power of transfer learning, it is possible to use pre-trained models with different types of systems. Therefore, transfer is an important concept in deep learning, and it arises from insufficient data and starting training from scratch. Transfer learning transforms learning from a pre-trained model to a new related model. So, it is a learner trained on data from different domains because sometimes it is difficult and expensive to train data with the traditional machine learning technique, which assumes training data in the same domain [15].

Our contribution

The following is a summary of this paper's contributions:

- We implemented the CAN communication protocol using the CAN communication toolbox in Simulink [16] and integrated it into an AV simulation model developed by MathWorks, Inc. [17]. This allows connected physical devices such as sensors, the adaptive cruise control (ACC) system, and actuators to interact and collaborate, called autonomous vehicle cyber-physical systems (AV-CPS).
- We generate the dataset from the AV-CPS and preprocess it by converting signals into images to be fed to the pre-trained CNNs.
- We implemented an intelligent intrusion detection system (IIDS) using eight pre-trained networks and performed each network's performance analysis. Our experiment found that GoogLeNet performed best because it recorded 99.47% based on the F1-score parameter.

Paper structure

The rest of this paper is structured as follows: Sect. 2 contains the literature review, which discusses the most recent works and the research gaps in the security of autonomous vehicles. Then, Sect. 3 presents the research methodology, including the implementation of the autonomous vehicle cyber-physical system (AV-CPS), and discusses the process of collecting preprocess of the dataset, followed by the findings and discussion in Sect. 4. Finally, the conclusions and remarks are drawn in Sect. 5.

Related research

The continued advancement in artificial intelligence, communication, and remote sensing have significantly improved the development cycle of smart cities and their applications and services. Several smart services have surfaced and industrialized recently to enhance the standard of living in smart cities, covering diverse sectors such as communication, cybersecurity, smart grids, healthcare, and transportation systems [18–20]. Much of the efforts were directed toward developing smart mobility and intelligent transportation systems such as autonomous vehicles [21]. Over 250 million automobiles will be connected to roadside units in a few years [22]. Despite this enormous growth of the autonomous vehicles industry, they are susceptible to a broad scale of cyberattacks with impacts ranging from minor control commands to strict control that threaten individuals' lives and well-being. Hence, various studies and systems have been suggested to examine, recognize, and alleviate the cyberattacks and threats against autonomous vehicle systems. The majority of the conducted studies were developed by coupling the different machine learning (ML) methods with cybersecurity practices to build security and defense systems.

In [23], an intelligent intrusion detection mechanism to secure external communications for autonomous vehicles was proposed and developed. The detection mechanism is based on a hybrid intelligent intrusion system that combines multi-layer perceptron (MLPs) with the overlapping proportional scores (POS) technique [24] and fuzzy sets to recognize the actions of connected, communicating autonomous vehicles. Specifically, their hybrid IDS utilizes the backpropagation neural networks to identify Denial of Service (DoS) attacks. Their experimental evaluation showed that their proposed detection showed high detection rates for DoS attacks in autonomous vehicles. However, their model has high inferencing overhead due to the computational processing through diverse subsystems such as the preprocessing subsystem, feature extortion subsystem with POS module, fuzzification subsystem [25] to reduce the features of data, MLP training subsystem, and finally, the detection subsystem (identify the traffic to either normal or anomaly).

In [26], the authors presented and implemented a detection method for false data injection in autonomous vehicles. Their system is composed of three subsystems. First, the false data injection (FDI) [27] subsystem, in which they inject simulated attacks into an autonomous vehicle. Second, the cyberattack dataset collection (CDC) subsystem generates and collects the dataset from a simulation model under two modes of operation (normal mode and attack mode). Third, the intrusion detection mechanism (IDM) subsystem employ the

long short-term memory (LSTM) deep networks [28] to detect cyberattack, which is FDI attacks targeting the control system of autonomous vehicles. Their IDS system categorizes the data sample as normal and abnormal. Their investigational evaluation proved the superiority of their model, scoring high detection rates outperforming other state-of-the-art models. However, their proposed system used only a simulated dataset without implementing the control communication system over autonomous vehicles.

In [29], the authors described a machine learning-based intrusion detection system (ML-IDS) developed mainly to minimize the risk of traffic disturbance and collisions triggered by the presence of cyber-attacks. Their proposed IDS can identify two types of cyberattacks commonly deliberated against connected autonomous vehicles: spoofing attacks and jamming attacks. The IDS mechanism was developed using four different learning techniques, including Random Forest (RF), k-nearest Neighbors (k-NN), One-Class Support Vector Machine (OCSVM), and Data Fusion (DF) in a cross-layer approach. Their experimental assessment showed that the based DF technique obtained the best performance factors, scoring more than 90% accuracy using training datasets with known and unknown attacks. However, the detection accuracy obtained by the author needs to be more competent, as it has been overcome by several other intelligent models, such as [30]. In the same context, the authors of [31, 32] proposed another ML-IDS to detect malicious traffic in the CAN bus network. Their proposed ML-IDS system employs a naïve Bayes algorithm and random decision trees to detect three types of cyber-attacks: impersonation attacks, DoS attacks, and fuzzy attacks. According to their experimental assessment, the authors conclude that their proposed ML-IDS is scalable and adaptable to various new attacks on autonomous vehicles. However, their model utilized imbalanced classes of the used dataset, which may affect the results attained for the performance evaluation indicators.

In [33], another machine learning-based intrusion detection system (ML-IDS) for autonomous vehicle communication is established on the realistic network dataset called the ToN-IoT dataset [34]. To reduce the number of features, the Chi-square (Chi2) method is used for feature selection [35]. Also, to avoid outweighing features with higher values over features with lower values, data normalization normalizes all numerical data records in the dataset. Moreover, since the ToN-IoT dataset is imbalanced, the Synthetic minority oversampling technique (SMOTE) [36] was used for class balancing. Besides, the model has been configured to provide binary classification (normal vs. anomaly) and multiclassification (normal, password attack, scanning, distributed denial of service (DDoS), data injection, backdoor, Cross-site Scripting (XSS), denial of service (DoS), and man-in-the-middle (MITM), and ransomware). To this end, the contributors have characterized the performance of eight supervised machine learning techniques: naive Bayes (NB), decision tree (DT), logistic regression (LR), support vector machine (SVM), k-nearest neighbor (kNN), random forest (RF), AdaBoost, and XGBoost techniques. Based on the simulation results, the XGBoost method outperformed other ML methods. However, their best model could perform better on sparse and unstructured data (such as outliers).

In [37], an automated cloud-based intrusion detection framework with continuous service availability for autonomous vehicles is developed and suggested to provide defense services at users' quality of service (QoS) and quality of experience (QoE) requirements. The proposed technique is developed by clustering autonomous vehicles into service-specific clusters, each with a cluster head to communicate with a trusted third party (TTP). This mediates the service between requesters and providers. Also, the proposed IDS comprises three modules, including traffic analysis, reduction, and classification (identifying good and bad requests). Specifically, their detection model employed the deep belief networks (DPN) for traffic reduction and decision tree techniques for classification purposes. Their validation process demonstrated the usefulness of their IDS, scoring high positive (around 99%) and low false detection rates (less than 1.6%).

In [38], a cost-effective, lightweight intrusion detection scheme was built to identify abnormalities in the autonomous vehicular system. The model design aimed to mitigate the risks of cyberattacks against the Internet of Vehicles (IoV) [39], which might cause fatal errors in vehicle control systems such as braking control, steering control, air conditioning control, and locking control elements. To do so, they suggested a model based on a three-layer neural network with a Softmax classifier to provide a binary detection of the input data records into either normal or abnormal or multi-classification into normal, reconnaissance attack, denial of service (DoS) attack, and fuzzing attack. They evaluate their IDS model on a simulated In-Vehicle Network (IVN) dataset originally generated from the control area network (CAN). They reported several evaluation outcomes, including detection accuracy, recall, precision, and F-1 score. Based on their comparative analysis, they concluded that their proposed scheme surpasses other classification schemes. However, their shallow model must provide accurate detection and classification for large-scale attack vectors

developed with minor mutation of previously developed attacks [40].

In [41], the authors focused on identifying malicious cyber-attacks targeting the electronic control units (ECUs) composing the autonomous vehicular system and connected via in-vehicle networks (controller area network-CAN). To that end, they proposed a hybrid anomaly-based intrusion detection system (HAIDS) using rule-based and supervised learning-based methods. Their model aims to attain a high identification ratio at minimal computational complexity. Their experimental setup comprised the collected CAN traffic from four different simulated vehicles. The rule-based part of the model was developed using three main rules, including Valid vehicle ID, Time Interval for message communication in CAN, and the valid data length code, which specifies the length of the messages in bytes. The machine learning part of the model was implemented as a three-layer neural network. As a result, they concluded that their hybrid IDS is effective and efficient in detecting anomalous over CAN communications.

Similarly, another hybrid anomaly-based intrusion detection system (HAIDS) employing rule-based IDS and machine learning IDS is suggested in [42]. In addition to the rule-based model, this system has characterized the performance of the supervised learning methods, viz., decision tree, random forest, and XGboost. As a result, they reported that their system could detect malicious CAN traffic with an accuracy of more than 90%. However, these proposed systems can not detect attacks that drop aperiodic messages that leverage the periodicity of CAN messages, which is still an open research problem.

Another noticeable research direction that has recently emerged is the use of blockchain technology to provide detection for several cyber-and physical attacks on the Internet of Things (IoT) in general [43] and in autonomous vehicles in specific [44, 45]. For instance, researchers in [44] focused on analyzing privacy and trust issues in autonomous transportation systems (ATS). They mainly investigated the cyberattacks on several communication techniques employed in autonomous vehicles, such as WLANs (Wireless Local Area Networks), WPANs (Wireless Personal Area Networks), WSNs (Wireless Sensor Networks), and RFID (Radio Frequency Identification). Therefore, they proposed a new IDS system (PChain) based on Blockchain Technology. PChain IDS protects IoT and ATS/ Vehicular Edge Computing (mainly autonomous vehicles). As a result, the model evaluation revealed that the detection accuracy rate changes with data size, which peaked at 95.5% for 10,000 data sizes and 40 training epochs. A similar tendency for precision and recall factors, which scored 94% and 95% for precision and recall, peaked at 10,000 data sizes and 40 training epochs. However, the researchers in this research have evaluated their model's performance on the KDDCup99 dataset [46], which comprises old common cyber-attacks that might be outdated in the current era. In the same context, the authors in [45] proposed a cooperative IDS system for autonomous vehicular networks tailored to the increased attack surface from common cyber-attacks. The proposed IDS system uses a decentralized federated-based methodology to decrease the resource utilization overhead of the main server by distributing the training load into distributed edge devices. To guarantee the security of the accumulation mechanism, blockchain is employed for storing and sharing the training loads. However, blockchain technology is vulnerable to cyber-attacks, such as ransomware attacks [47].

Furthermore, authors in [61] investigated anticipating and adjusting to users' interests and preferences in location-based social networks using copious amounts of user check-in data from Internet of Things (IoT) devices like cell phones. One important component of the Augmented Intelligence of Things (IoT) is the recommendation of successive points of interest (POIs), which is examined. Limitations of existing methodologies are emphasized and examined, including recurrent neural network-based approaches and graph neural network-based methods. The abstract suggests an Interaction-enhanced and Time-aware Graph Convolution Network (ITGCN) for successive POI suggestions to overcome these drawbacks. ITGCN integrates a self-attention aggregator to embed high-order connectivity into node representation and an enhanced graph convolution network for dynamic representation learning. The system aims to help corporate management anticipate user preferences so that better development and planning may occur. According to their experimental results, ITGCN performs better regarding suggestion accuracy than current approaches. To sum up, the following table, Table 1, provides a very short summary of the key points in the related works.

In [62], the authors addressed how the growing number of Connected and Autonomous Vehicles (CAVs) exposes Internet of Vehicles (IoV) environments to cyberattacks. The study suggests an Intelligent Intrusion Detection System (IIDS) that uses a modified Convolutional Neural Network (CNN) with hyperparameter tuning to address this issue. In a 5G Vehicle-to-Everything (V2X) setting, the IIDS efficiently identifies and classifies malevolent Autonomous Vehicles (AVs), assisting in traffic safety monitoring and collision avoidance. According to experimental results, attacks can be detected with 98% accuracy. In the same context, the authors of [63] investigated the increasing risk of cyberattacks on in-car

Table 1 A very short summary of the key points in the related works

Ref.	Key Attributes	Strengths	Weaknesses
[23]	- Hybrid IDS using MLPs and POS techniques - Detection of DoS attacks in autonomous vehicles	- High detection rates for DoS attacks - Experimental validation	- High inferencing overhead - Computational processing through diverse subsystems
[26]	- Detection method for false data injection - Use of LSTM deep networks	- Superior detection rates - Categorization of data samples as normal or abnormal	- Use of simulated dataset without real-world implementation
[29]	- ML-IDS to minimize traffic disturbance and collisions - Identification of spoofing and jamming attacks	- Four learning techniques used - DF technique achieved over 90% accuracy	- Detection accuracy needs improvement compared to other models
[31, 32]	- ML-IDS for detecting malicious traffic in the CAN bus network - Naïve Bayes and random decision trees used	- Scalable and adaptable to various attacks	- Utilization of imbalanced classes in the dataset
[33]	- ML-IDS for autonomous vehicle communication - Based on ToN-IoT dataset - Use of the Chi-square method for feature selection	- Performance of eight supervised ML techniques evaluated - XGBoost outperformed other methods	The best model may need more sparse and unstructured data
[37]	- Cloud-based intrusion detection framework - Clustering of autonomous vehicles - Use of DPN and decision tree techniques	- Continuous service availability - High positive and low false detection rates	- Specific to cloud-based detection
[38]	- Cost-effective, lightweight intrusion detection scheme - Three-layer neural network with Softmax classifier	- Detection accuracy, recall, precision, and F-1 score reported - Outperformed other classification schemes	- Shallow model may struggle with large-scale attack vectors
[41]	- Hybrid anomaly-based IDS for electronic control units - Rule-based and supervised learning-based methods	- High identification ratio - Minimal computational complexity	- Specific to anomalous CAN communications
[42]	- Hybrid anomaly-based IDS with rule-based and machine-learning IDS - Decision tree, random forest, and XGBoost used	- Detection of malicious CAN traffic with over 90% accuracy	- Unable to detect attacks leveraging the periodicity of CAN messages
[44]	- PChain IDS based on Blockchain Technology - Focus on privacy and trust issues in autonomous transportation systems	- Evaluation revealed high detection accuracy - Use of blockchain for security	- Evaluation based on an old dataset of common cyber-attacks
[45]	- Cooperative IDS for autonomous vehicular networks - Decentralized federated-based methodology - Use of blockchain for storing and sharing training loads	- Decreased resource utilization overhead - Distributed edge devices for training load	- Vulnerability of blockchain to cyber-attacks like ransomware
[61]	- Exploration of user check-in data for POI recommendations - Critique of recurrent and graph neural network-based methods	- Introduction of ITGCN for successive POI suggestions - Experimental results show improved accuracy	- Limitations of existing methodologies highlighted
[62]	- Addresses cybersecurity risks in IoV due to CAVs - Proposes IIDS with modified CNN for AV classification - Operates in a 5G V2X environment	- Efficiently identifies and classifies malicious AVs - Enhances traffic safety monitoring and collision avoidance - Achieves 98% accuracy in attack detection	-Limited Security Measures - Focusing on specific CNN hyperparameters may limit its adaptability to emerging cyber threats
[63]	- Focuses on cyberattacks on in-car networks due to electronics integration - Targets vulnerabilities in the CAN bus - Proposes DCNN-based IDS for the CAN bus	- DCNN learns network traffic patterns without human feature design - Outperforms traditional machine-learning techniques - Demonstrates lower false negative and error rates	- Limited information on the scale or diversity of experiments

Table 1 (continued)

Ref.	Key Attributes	Strengths	Weaknesses
[64]	- Emphasizes IDS necessity for the vulnerable CAN bus.—Introduces GIDS, a GAN-based IDS for in-vehicle networks - GIDS learns and identifies unknown attacks with regular data	- GIDS achieves excellent detection accuracy for unknown assaults - Addresses the lack of security measures in the CAN bus	- Needs more details on the specific architecture of GIDS
[65]	- Discusses limitations of RNNs in in-vehicle intrusion detection - Proposes TCAN-IDS, a Temporal Convolutional Network with Global Attention - Addresses real-time monitoring challenges	- TCAN-IDS encodes 19-bit characteristics for real-time monitoring - Global attention mechanism enhances feature extraction - Demonstrates strong detection performance on known attack datasets	- No details were provided on the scale or diversity of experiments
[66]	- Highlights difficulties in intrusion detection for vehicle communications - Proposes STC-IDS for spatial–temporal correlation - Addresses challenges in local feature consideration and poor multi-feature mapping	- STC-IDS encodes spatial and temporal interactions simultaneously - Outperforms baseline approaches - Achieves lower false alarm rates while maintaining efficiency	- Needs more specific details on the architecture of STC-IDS

networks due to the integration of electronics into contemporary cars, which is covered in this abstract. Commonly found in automobiles, the controller area network (CAN) is vulnerable to assaults since it lacks crucial security measures. The study suggests a deep convolutional neural network (DCNN)–based intrusion detection system (IDS) specially designed for the CAN bus. Without human feature design, the DCNN learns network traffic patterns, simplifying the architecture and optimizing for excellent detection performance. Based on real-world car datasets, experimental results demonstrate that the suggested IDS performs better than traditional machine-learning techniques, with notably lower false negative and error rates.

In another noticeable research, in [64], the researcher emphasized the necessity of an efficient Intrusion Detection System (IDS) by highlighting the vulnerability of the Controller Area Network (CAN) bus in automobiles due to its lack of security measures. Vehicle networks with limited known attack signatures might not fit traditional internet-based intrusion detection systems well. The suggested remedy is a new intrusion detection system (IDS) model dubbed GIDS (GAN-based Intrusion Detection System) that uses Generative Adversarial Nets, a deep learning model. With just regular data, GIDS can learn and identify unknown assaults. Experimental findings address the problem of guaranteeing safety in in-vehicle networks by demonstrating GIDS's excellent detection accuracy for four unknown assaults. In [65], the authors have discussed the limitations of recurrent neural networks (RNN) in developing efficient intrusion detection systems for in-vehicle networks are discussed in this abstract. These limitations originate from RNNs' intricate structure and high processing costs. Additionally, it mentions that temporal linkages are difficult for convolutional neural networks (CNN) to capture and that important regions have insufficient feature representation. To solve these problems, the research suggests a novel model named TCAN-IDS (Temporal Convolutional Network with Global Attention). Real-time monitoring is made possible by TCAN-IDS, which encodes 19-bit characteristics of data fields and arbitration bits into a message matrix. By concentrating on important areas, the global attention mechanism enhances feature extraction. TCAN-IDS has demonstrated strong detection performance on attack datasets that are known to exist, according to experimental results. This means that it can be used for real-time monitoring and to maintain the delicate balance between information security and preventing unauthorized intrusions.

Furthermore, in [66], the authors highlighted the difficulties caused by various attack techniques while underlining the significance of intrusion detection for vehicle communications security. The limits of previous approaches, which consider local characteristics or map multi-features poorly, are critiqued. Spatial and temporal interactions are simultaneously encoded by the encoding-detection architecture of the proposed model, STC-IDS (Spatial–Temporal Correlation Intrusion Detection System). Attention-based convolutional networks and attention-long short-term memory produce strong spatial–temporal attention features for anomaly classification. Both single- and multi-frame architectures have specific benefits. Empirical investigations on real-world vehicle assault datasets show that STC-IDS outperforms baseline approaches with automatic hyperparameter selection based on Bayesian optimization, delivering lower false-alarm rates while maintaining efficiency.

While the above-stated systems are established and focused on developing Attack-Aware systems [48] utilizing different computational intelligence schemes such as fuzzy inference systems (FISs), neural network systems (NNS), and machine learning systems (MLS) over predefined accumulated datasets that are composed using the most conventional attributes for the common cyberattacks of communication networks on the IoT, CPS, and others, nevertheless, these systems do not support the identification of new real-time cyberattacks targeting the autonomous vehicle-cyber physical system's controller area network (CAN) communication system. In this research, we improve the security of autonomous vehicle control by developing a high-performance intelligent intrusion detection system (IIDS) using non-traditional machine learning techniques.

Particularly, we first develop our autonomous vehicle cyber-physical systems (AV-CPS) by implementing the controller area network (CAN) communication protocol and then integrating it into an autonomous vehicle simulation model. This, in turn, enables the other connected physical devices (e.g., sensors and actuators) to communicate and collaborate (C&C) successfully. Second, we produce and collect our novel dataset from launching AV-CPS in normal and attack modes. The generated dataset comprising of normal data samples accumulated from the normal operational mode of AV-CPS and false data samples injected by the attacker then undergoes consecutive preprocessing operations to end up with all samples transformed into unitized images that the deep neural networks can process. Finally, we implement an intelligent intrusion detection system (IIDS) using the transfer learning process from pre-trained deep convolutional networks (DCNNs). Specifically, we characterized the performance of eight DCNNs, including InceptionV3 CNN, ResNet-50 CNN, ShuffleNet CNN, MobileNetV2 CNN, GoogLeNet CNN, ResNet-18 CNN, SqueezeNet CNN, and AlexNet CNN. Our simulation results demonstrated high detection performance for our IIDS-based GoogLeNet model after we validated it with other implemented DCNNs and existing models in the same study area.

Methodology

This section explains the AV simulation scheme used in this research. Also, it represents the process of using the CPS concept with the selected AV simulation. This is accomplished by implementing and integrating communication network nodes into the AV simulation, and we named the new model the autonomous vehicle cyber-physical system (AV-CPS). Additionally, this section explains the procedure for generating the dataset from the AV-CPS simulation model. Finally, it shows the process of using transfer learning.

AV Simulation scheme

A simulation is a software-based model that can be used to study and evaluate a model's performance before it reaches the production stage [49]. There are several benefits of using a simulation model compared with an actual model, such as less cost-effectiveness and simplicity in implementation, testing, and maintenance [50]. The simulation model used in this research is a self-driving car system consisting of a lead vehicle and an ego vehicle (self-driving car). In ideal conditions, the ego vehicle should maintain its distance from the lead vehicle using the ACC. Therefore, the ego vehicle should keep track of the position of the lead vehicle. This study focuses on the ego vehicle, which consists of three essential components: ACC, position sensor, and velocity sensor, as shown in Fig. 2. The position sensor senses the position of the lead vehicle and ego vehicles' positions. Furthermore, the velocity sensor records the velocity of the lead and ego vehicles. The sensor measurements are sent to the ACC to adjust the speed of the ego vehicle when following the lead vehicle.

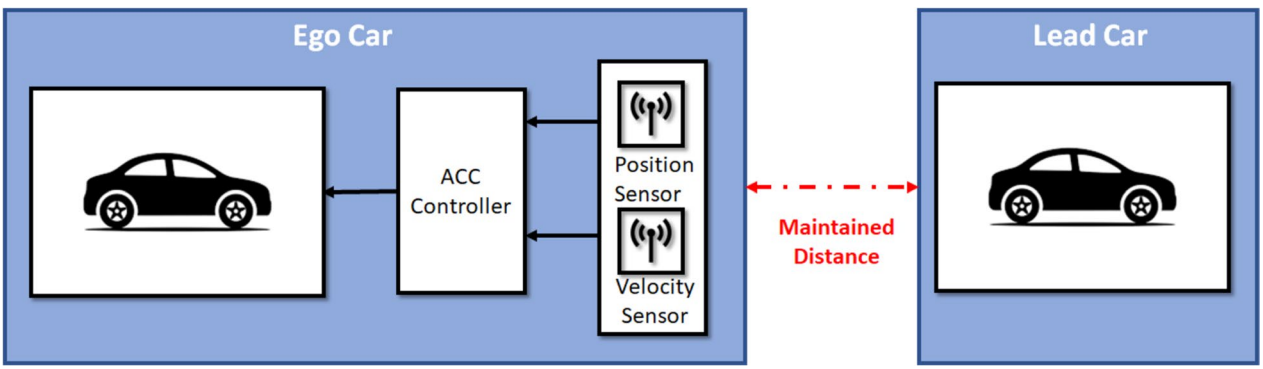

Fig. 2 AV simulation scheme

CAN communication network

MathWorks AV simulation does not include a communication system component; therefore, to apply the CPS concept, we implemented and integrated a communication system based on CAN protocol using the vehicle network toolbox built on Simulink [16]. The vehicle network toolbox contains techniques and tools to design, analyze, architect, simulate, and validate communications systems. The toolbox has several components: CAN communication, CAN Flexible Data (FD) communication, J1939 communication, and Universal Measurement and Calibration Protocol (XCP) communication. This research concentrates on using the CAN communication component to build the communication system of the AV-CPS. Table 2 lists the CAN block used, and Fig. 3 shows the sending and receiving messages of the CAN communication subsystem. Initially, the signal is packed to the CAN message stander using the CAN pack; then, the CAN message is transmitted to the assigned CAN device using the CAN transmit component. The CAN configuration configures particular CAN devices' parameters for sending and receiving CAN messages. Finally, the CAN message is received from the particular CAN device, and the CAN unpack is used to unpack the CAN message to signals.

Table 2 CAN communication component

CAN Block	CAN Configuration
CAN Pack	Signals should be packed within a CAN message
CAN Transmit	Send a CAN message to a particular CAN device
CAN Configuration	Configure parameters of particular CAN devices for sending/receiving messages
CAN Receive	Receive CAN messages from the particular CAN device
CAN Unpack	Unpacked CAN message to signals

Autonomous vehicle cyber-physical system

The AV-CPS architecture implemented in this research comprises the following subsystems: sensors, two CAN communication nodes, a controller, and actuators. Nodes A and B receive and send signals between the AV subsystem, as shown in Fig. 4. Nodes A and B are integrated to simulate the activity of the CAN communication within the AV-CPS. Therefore, node A's functionality is to receive and send the following signals:

- The actual location of the ego vehicle (from the sensor).
- The actual position of the lead vehicle (from the sensor).
- The actual speed of the ego vehicle (from the sensor).
- The actual speed of the lead vehicle (from the sensor).
- The time gap (constant value).
- The desired speed (constant value).

The actual position of the ego vehicle is measured in meters, and the velocity is measured in m/s. The time gap between the lead vehicle and the ego vehicle is equal to 1.4 s. The desired speed is equal to 30 m/s. After the signals are transmitted to the ACC, it is responsible for producing a control signal to adjust the ego vehicle's speed concerning the desired speed and the position of the lead vehicle. Finally, the ACC output is received and sent to the actuators by node B. The actuators convert the signal to mechanical movement to accelerate or reduce the speed. We showed a single closed-loop operation of the simulation, and those steps are repeated until the end, which runs for 81 s.

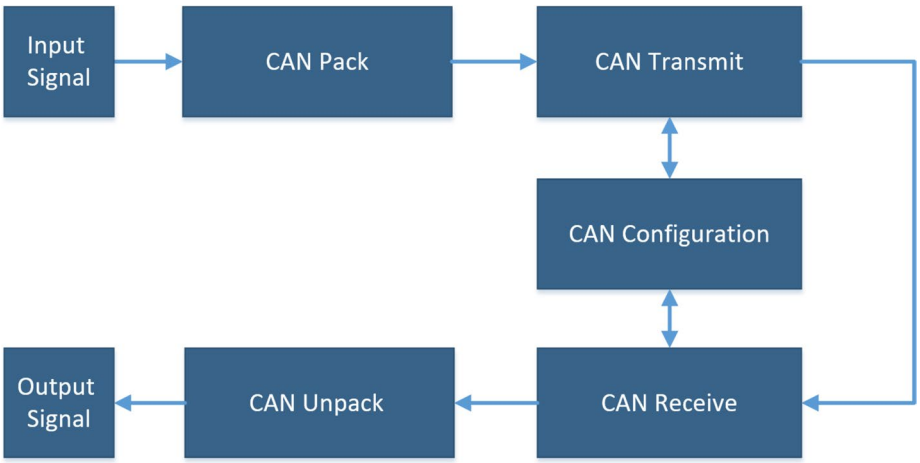

Fig. 3 CAN send and receive messages

Generating dataset

As shown in Fig. 5, it is assumed that a threat actor compromised node A. Thus, the threat actor inserted inaccurate data into the position sensor of the ego vehicle through node A. Therefore, the ACC received fault data about the position of the ego vehicle, and as a result, the ACC produced imperfect control signals. Figure 4 and Fig. 5 represent two different scenarios. Figure 4 shows the normal status when there is no cyberattack, whereas Fig. 5 illustrates the anomaly status when there is a cyberattack. More information about the implementation of the cyberattack was presented in our previous research [26]. The raw dataset is 1-dimensional, and its size is 80,000. The dataset is balanced; therefore, 40,000 is normal, and the rest is attack data. The dataset consists of four features: (1) the actual position, (2) the actual velocity of the ego vehicle, (3) the actual position, and (4) the actual velocity of the lead vehicle. Table 3 lists the raw dataset along with its unit.

To prepare the pre-trained neural network input, we must transform the numerical 1-dimensional data into 2-dimensional data (images). Figure 6 illustrates the steps undertaken to convert signals into images. In step 1, the AV-CPS simulation runs. Step 2 records the response of the features as mentioned earlier as numerical 1-dimensional data in a matrix. Step 3 then reshapes this stored data from a 1D matrix to a 2D matrix. Step 4 involves saving the 2D matrix as an image; each image has a size of 4×81. We have the size of 4×81 because we have four features, and the simulation runs for 81 s each time. Finally, step 5 stores the resulting normal and anomaly images in separate folders.

Algorithm 1 illustrates how the 1-dimensional data was converted to 2-dimensional data (image). Initially, 'im_counter' is set to 0 to name the image. The 'start_row' and 'last_row' variables are used as counters because we aim to combine all four dataset rows. Subsequently, the normal and attack data are loaded for use. The 'normal' directory contains images with normal data, and the 'attack' directory is created to hold attack images. The while loop starts with one and continues up to the length of the data source, either normal or attack. Consequently, 20 thousand images will be created: 10 thousand labeled as normal and 10 thousand labeled as attack, and each image will be created in jpg format.

1:	**Initialize** img_counter to 0
2:	**Initialize** start_row to 1
3:	**Initialize** last_row to 4
4:	**Load** normal_data
5:	**Load** attack_data
6:	**Set** mycase to either "normal" or "attack."
7:	**Create** a directory named after mycase if it does not exist.
8:	**While** start_row is less than or equal to the size of the selected data source
9:	**If** mycase is "normal," then
10:	**Set** x to a subset of normal data from index start_row to last_row
11:	**Reshape** x into a 4x81 array named image.
12:	**Increment** img_counter by 1
13:	**Create** a jpg image named img_counter.jpg and store it in the normal folder.
14:	**Else, If** mycase is "attack," then.
15:	**Set** x to a subset of attacked data from index start_row to last_row
16:	**Reshape** x into a 4x81 array named image.
17:	**Increment** img_counter by 1
18:	**Create** a jpg image named img_counter.jpg and store it in the folder attack.
19:	**EndIf**
20:	**Increment** last_row by 4
21:	**Increment** start_row by 4
22:	**End While**

Algorithm 1 Convert 1-D data to a 2-D image

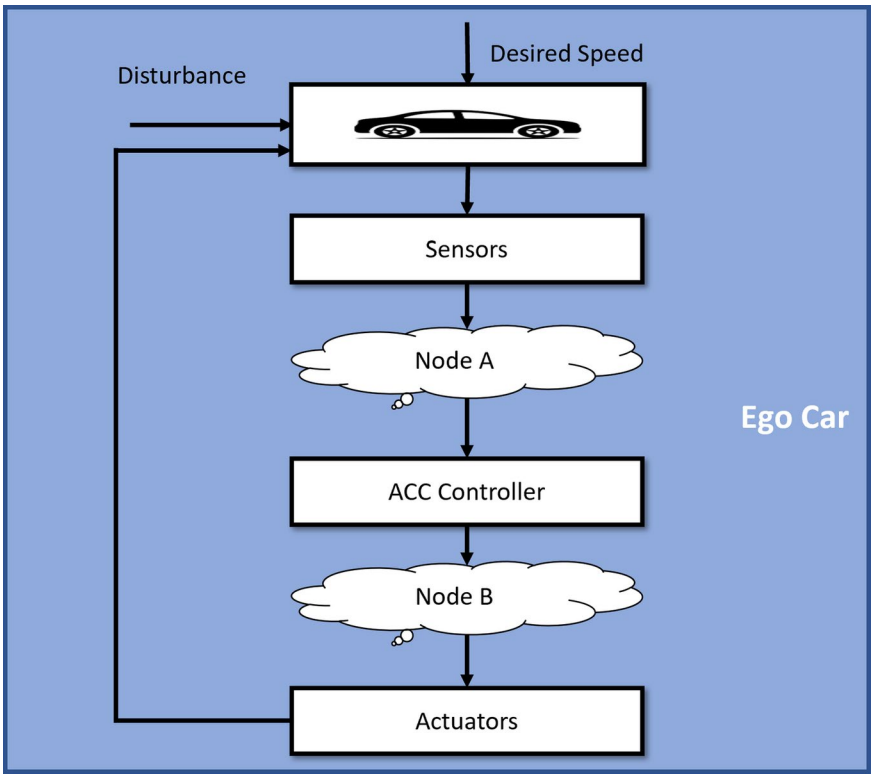

Fig. 4 Autonomous vehicle cyber-physical system(AV-CPS)

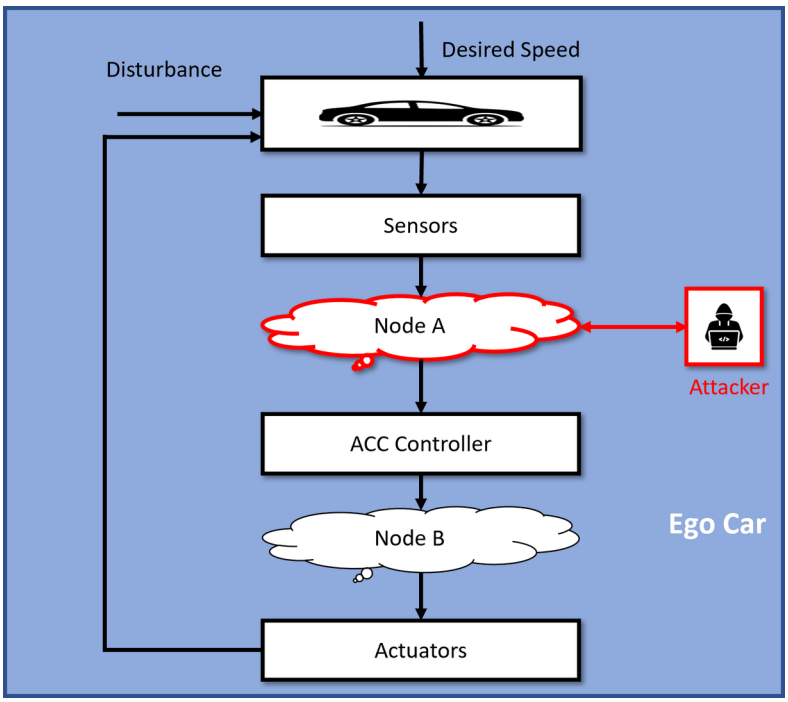

Fig. 5 Cyberattack vs. autonomous vehicle CPS model

Table 3 1-Dimensional dataset

Feature	Vehicle	Unit
Actual position	Ego vehicle	Meter
Actual velocity	Ego vehicle	Meter/Second
Actual position	Lead vehicle	Meter
Actual velocity	Lead vehicle	Meter/Second

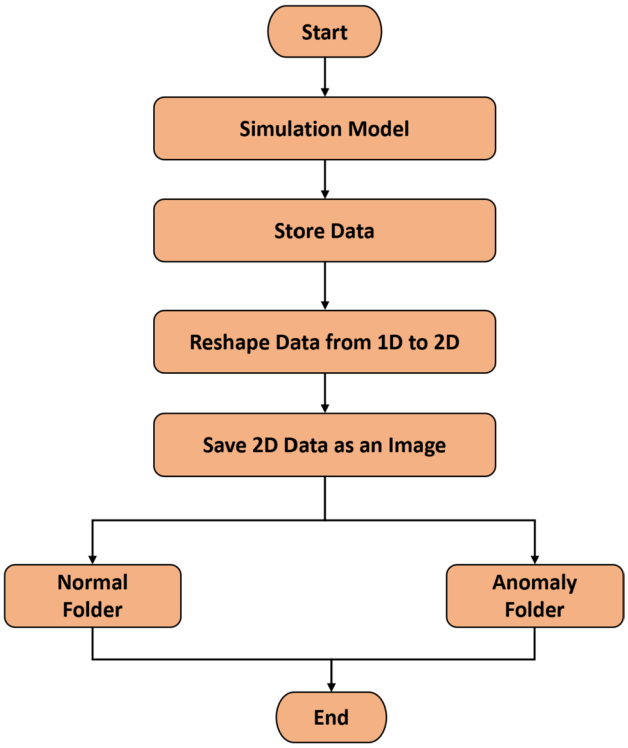

Fig. 6 Conversion into image steps

Figure 7 highlights the process of preparing images for each pre-trained neural network model used in this research. In the beginning, the images are imported into MATLAB. The original size of the images is 4×81, but to ensure compatibility with each model, each image is resized to match the input size of the specific model. This resizing is performed by MATLAB using the augmentedImageDatastore function.

Figure 8 illustrates the process of the proposed IIDS. After the data is received from the CAN protocol, it will be sent to the IIDS for scanning the traffic. The 1-dimensional data is converted to an image and transmitted to the pre-trained CNN model. The CNN is responsible for detecting whether there is an attack or not.

Transfer learning

Transfer learning is an important concept in deep learning, and it arises from insufficient data and starting training from scratch [15]. The proposed work utilizes transfer learning by leveraging pre-trained models to enhance the IIDS performance for AV-CPSs. Transfer learning involves using knowledge gained from solving one problem (in this case, pre-trained models trained on large-scale datasets) to improve the performance on a different but related problem, detecting cyberattacks on AV-CPSs as depicted in Figs. 9 and 10 which illustrate the architecture of the pre-trained models used in this research named inceptionV3, resNet-50, shuffleNet, mobileNetV2, GoogLeNet, ResNet-18, squeezeNet, and alexNet. The Relu layer activates to omit any negative values from the images and replace them with zeros. A Pooling layer serves as a filter to reduce the size of the input image. Therefore, Relu and Pooling layers reduce

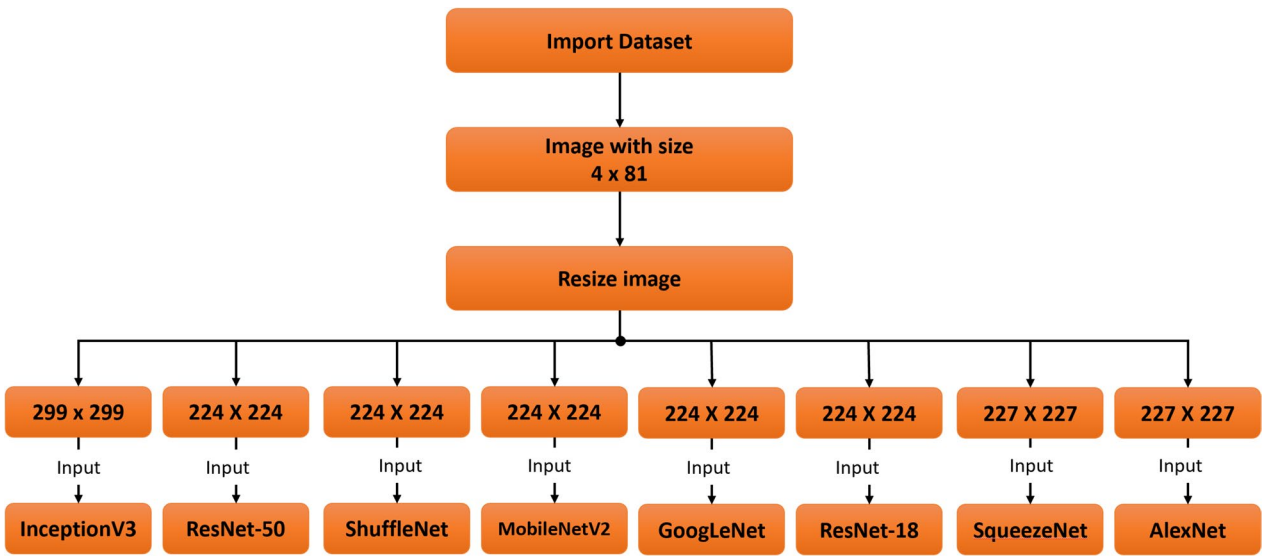

Fig. 7 Image resizing process

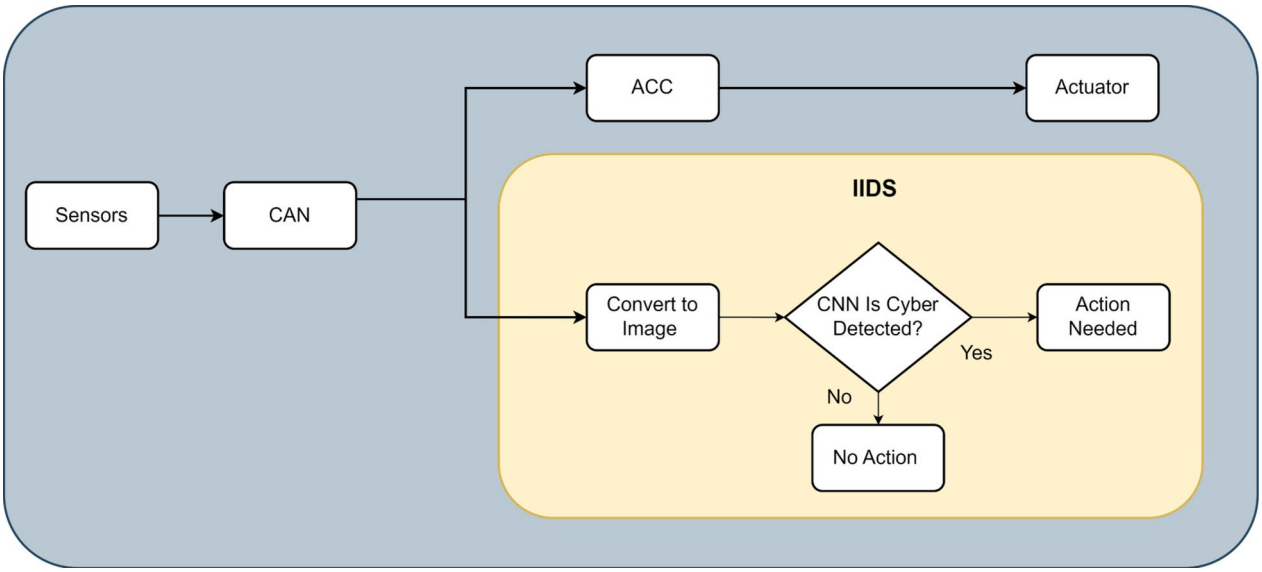

Fig. 8 IIDS procedure

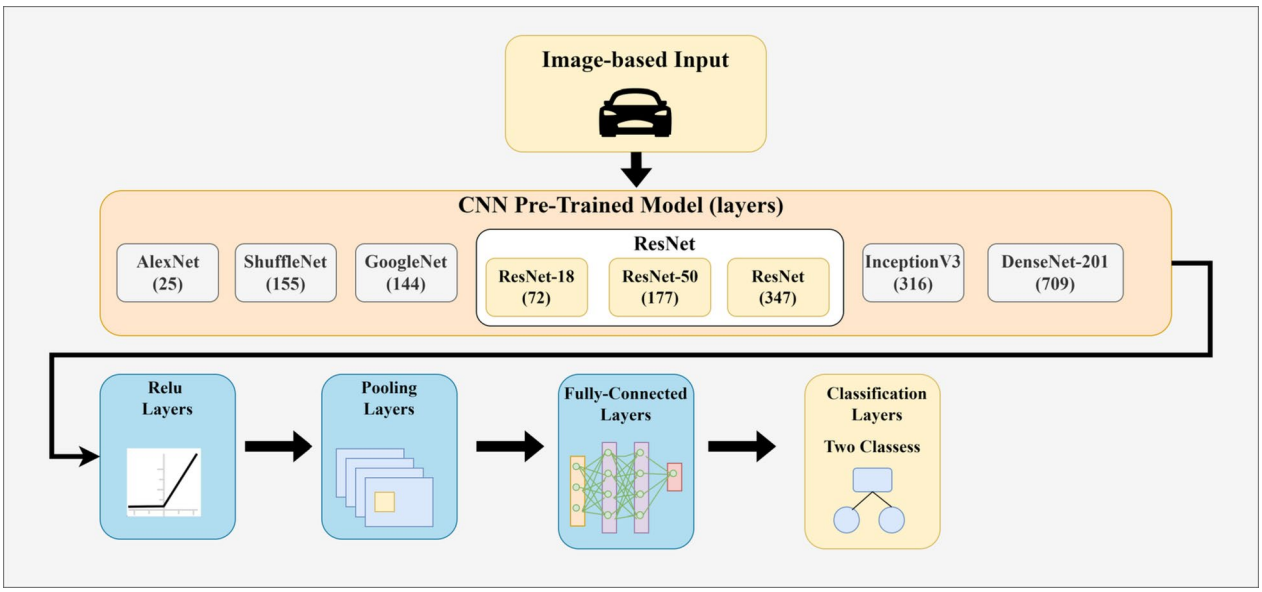

Fig. 9 CNN Pre-trained model

the computation costs. The Fully connected layer is used by all pre-trained models except squeezeNet, which uses a Convolutional 2D layer, and they help to classify images correctly [51]. Table 4 summarizes each model ordered by the number of layers [52]. The final layer of each model was altered to serve our purpose. For example, in inceptionV3, we replaced the fully connected layer and the classification layer to produce only two outputs (normal, anomaly).

This research used eight pre-trained CNNs; therefore, the generated dataset was trained, tested, and validated with each network.

Results and discussion

This section discusses the experimental setup, such as the software and hardware used to perform this research's experiments. Also, the results and discussion of the research findings were investigated.

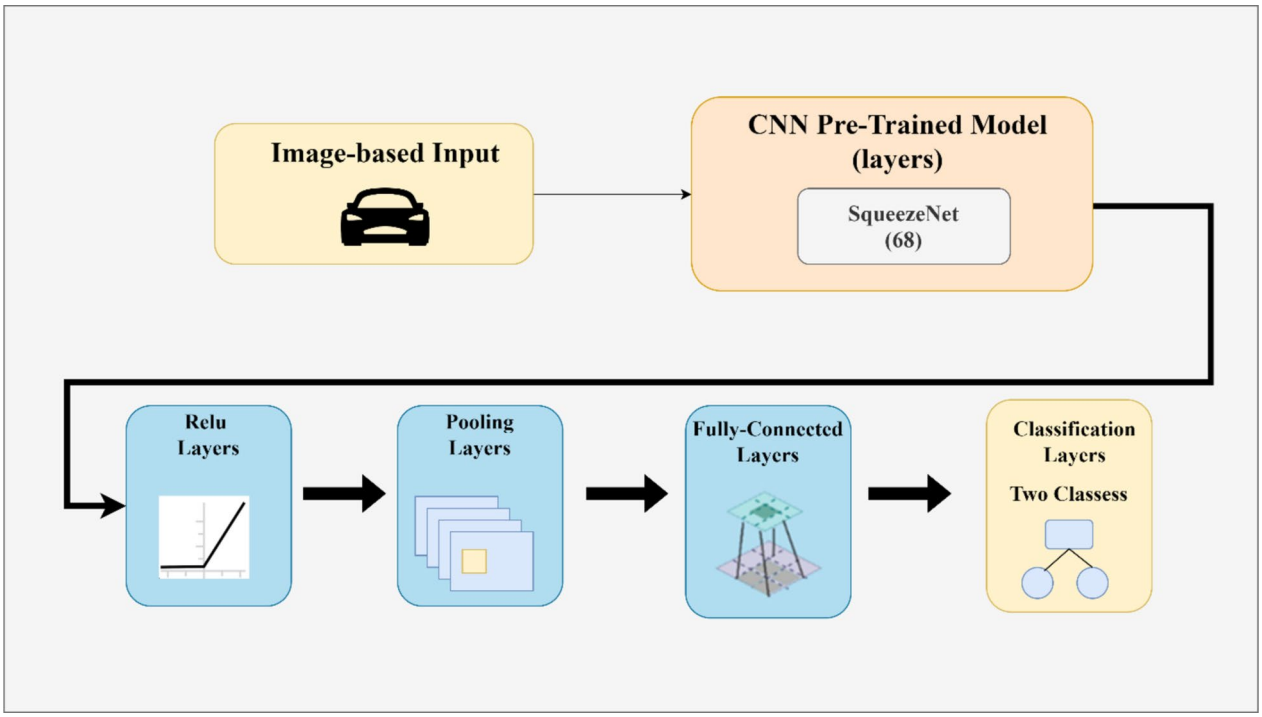

Fig. 10 SqueezeNet layer architecture

Table 4 Summary of pre-trained CNN models used in this research

Model Name	Depth	Number of Layers	Image Size	Replace Final Layer
InceptionV3	48	316	299 X 299	Fully connected layer, Classification layer
ResNet-50	50	177	224 X 224	Fully connected layer, Classification layer
ShuffleNet	50	173	224 X 224	Fully connected layer, Classification layer
MobileNetV2	53	155	224 X 224	Fully connected layer, Classification layer
GoogLeNet	22	144	224 X 224	Fully connected layer, Classification layer
ResNet-18	18	72	224 X 224	Fully connected layer, Classification layer
SqueezeNet	18	68	227 X 227	Convolution2dLayer, Classification layer
AlexNet	8	25	227 X 227	Fully connected layer, Classification layer

Experiment

The experiments were performed using MATLAB and Simulink. MATLAB is a high-level programming language platform, and Simulink is a MATLAB model-based design platform [53]. The AV simulation model was developed by MathWorks using MATLAB and Simulink. However, this research implemented the CAN component protocol using the Simulink network toolbox, which was then integrated into the AV simulation. We used MATLAB to implement and test the pre-trained CNNs. We conducted the training and testing

Table 5 Summary of components used to perform the experiments

Components	Type	Description
MATLAB	Software	Programming language platform
Simulink	Software	Model-based platform
CAN	Software	Simulink Network Toolbox
CPU	Hardware	Intel® Core™ i7-9750H
Memory	Hardware	16.0 Gigabytes
GPU	Hardware	NVIDIA GeForce RTX 2070 GDDR6 @ 8 Gigabytes

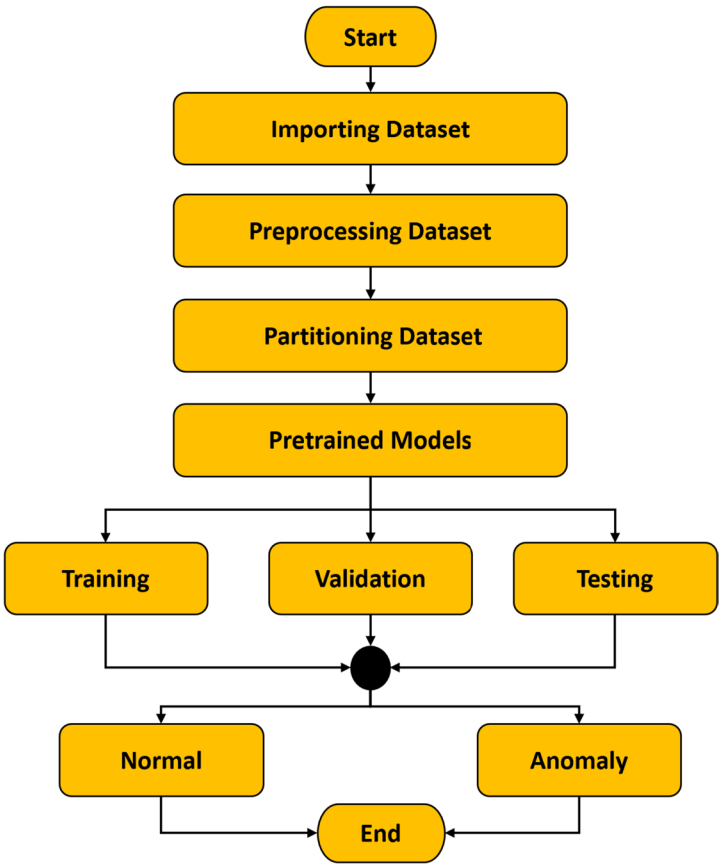

Fig. 11 Overall steps of the experiment

procedure using a computer system with a Graphics processing unit (GPU) to reduce the computation time and increase the experiment's performance. Table 5 summarizes the software and hardware used in this research.

Figure 11 summarizes the overall steps of our experiments used in this research. In the beginning, the dataset was imported to the MATLAB namespace, and as mentioned, the dataset was stored in two folders: normal and anomaly. Then, the dataset was preprocessed. Therefore, all images were resized to fit the appropriate input size of each pre-trained network. Each pre-trained model expected two class outcomes, anomaly and normal. The dataset was split into two parts: 70% of the images were used for training and 30% for testing and validation. The data size was 20,000 images; 10,000 was normal, and 10,000 was anomalous. A fivefold cross-validation technique was used to ensure the validity of our training process. Finally, the expected output of each model is either normal or anomalous. Normal means there is no attack and anomalous means there is an attack.

Result and evaluation

The detection outcomes of the eight pre-trained models used in this research were analyzed based on precision, recall, f1-score, and accuracy classification as follows [26]:

$$\text{Precision} = TP/(TP + FP)\text{x}100 \tag{1}$$

$$\text{Recall} = TP/(TP + FN)\text{x}100 \tag{2}$$

Table 6 Accuracy performance outcomes

Pre-trained	Precision	Recall	F1-Score	Accuracy
GoogLeNet	100.00%	98.94%	99.47%	99.47%
AlexNet	100.00%	98.85%	99.42%	99.42%
SqueezeNet	100.00%	98.78%	99.39%	99.38%
InceptionV3	100.00%	98.75%	99.37%	99.37%
ResNet-50	100.00%	98.75%	99.37%	99.37%
ShuffleNet	100.00%	98.62%	99.30%	99.30%
MobileNetV2	100.00%	98.62%	99.30%	99.30%
ResNet-18	100.00%	98.59%	99.29%	99.28%

Table 7 Performance of recent existing methods used with AV systems

Research Paper	Dataset	Methods	Performance	Metric
Al-Haija et al. [55]	DAWN2020 and MCWRD2018	ResNet-50	98.41%	FScore
Abd et al. [56]	Car Test-Bed and Network	ANN	92.10%	Accuracy
GAD et al. [57]	ToN-IoT	XGBoost	98.70%	FScore
Pascale et al. [59]	Carla simulation, KIA SOUL	Bayesian network	97.80%	FScore
Yang et al. [60]	Car-Hacking and CICIDS2017	Pre-trained CNNs	99.25%	FScore
Jeong et al. [58]	The AVTP intrusion	CNN	99.27%	FScore
Proposed Models	**AV-CPS**	**GoogLeNet**	**99.47%**	FScore

$$\text{FScore} = 2 * (\text{Precision} \times \text{Recall})/((\text{Precision} + \text{Recall}))\text{x}100 \quad (3)$$

$$Accuarcy = (TP + TN)/(TP + TN + FP + FN)\text{x}100 \quad (4)$$

TP is a true positive that calculates the number of normal images classified correctly. FP is a false positive that calculates the number of normal images classified incorrectly. FN refers to a false negative that calculates the number of abnormal images classified incorrectly. Finally, TN is a true negative that calculates the number of abnormal images classified correctly [54]. Table 6 represents the calculation accuracy of the pre-trained models based on four metrics of accuracy analysis. While all pre-trained models have approximately comparable performance results, GoogLeNet has an outperformed performance compared with other pre-trained models. The precision parameter has an identical value of 100.00% because every pre-trained model could classify every "normal image" as normal. However, the value of the recall parameter range from 98.94% to 98.59% due to several "anomaly image" being classified as normal. F1 score depends on parameters precision and recall, as shown in Eq. 3, and accuracy classification was calculated using Eq. 4.

To validate our work, we compared the performance outcomes of this research with recent existent IDS methods used with AV systems. Overall, pre-trained CNNs such as research 1,6 and 7 scored better than others, such as ANN and Bayesian networks, as listed in Table 7.

Conclusions and remarks

In conclusion, this research proposed an intelligent intrusion detection system (IIDS) to detect cyberattacks targeting physical components of an AV through controller area network CAN. Firstly, the CAN was implemented and integrated into an AV simulation developed by MathWorks to apply the CPS concept. Therefore, the new system is called an autonomous vehicle cyber-physical system (AV-CPS). Secondly, the dataset was generated from the AV-CPS and preprocessed by converting signals into images to be fed to pre-trained CNNs. Thirdly, eight pre-trained networks were implemented: InceptionV3, ResNet-50, ShuffleNet, MobileNetV2, GoogLeNet, ResNet-18, SqueezeNet, and AlexNet, and the performance analysis of each network was discussed. Our experiment found that GoogLeNet performed best because it recorded 99.47% based on the F1-score parameter. This research's resilient security concept can be used and applied to any CPS framework because each component of the system (AV-CPS) was built based on block architecture. Therefore, each subsystem, i.e., controller, sensors, actuators, and communication nodes, is independent and can be a breakdown. For feature work, we recommend applying the architecture of our system (AV-CPS) with different CPS domains, such as smart grids and drones.

Limitations

Our work primarily focuses on developing an IIDS by employing a transfer learning approach, specifically using pre-trained neural networks. The IIDS developed in this research, which is expected to collaborate with the ACC, aims to detect the network traffic locally (within the AV) emanating from sensors assumed to be compromised by attackers. Therefore, the IIDS is designed to scan network traffic transferred by the CAN model that is entering the ACC model. The anomaly detection technique conducted by the IIDS is confined to the data read by sensors; however, cyberattacks may be executed through various other components, a topic warranting future research. Additionally, researchers might consider designing an intelligent intrusion prevention system (IIPS) to mitigate the effects of cyberattacks.

Acknowledgements

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant No. IFPIP: 622-611-1443. Therefore, the authors acknowledge DSR's technical and financial support with thanks.

Authors' contributions

Conceptualization, A. A. A.; methodology, A. A. A. and Q. A. A-H.; software, A. A. A. and B. A.; validation, Q. A. A-H. and A. A. Q..; formal analysis, Q. A. A-H.;

investigation, A. A. A. and R. A. S.; resources, A. A. A. and B. A.; data curation, B. A., A. A. Q, and R. A. S.; writing—original draft preparation, A. A. A., Q. A. A-H, B. A., A. A. Q, and R. A. S..; writing—review and editing, A. A. A. and Q. A. A-H.; visualization, A. A. A., Q. A. A-H, B. A., A. A. Q, and R. A. S.; supervision, Q. A. A-H; Project Administration, A. A. A; funding acquisition, A. A. A. All authors have read and agreed to the published version of the manuscript.

Funding
This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant No IFPIP: 622–611-1443.

Availability of data and materials
The data will be made available upon request/acceptance.

Declarations

Ethics approval and consent to participate
Not applicable.

Competing interests
The authors declare no competing interests.

Received: 22 November 2022 Accepted: 5 December 2023
Published online: 20 December 2023

References

1. Cao Y, Xiao C, Cyr B, Zhou Y, Park W, Rampazzi S et al (2019) Adversarial sensor attack on LiDAR-based perception in autonomous driving. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, p 2267–2281. https://doi.org/10.1145/3319535.3339815
2. Jeong Y, Son S, Jeong E, Lee B (2018) An integrated self-diagnosis system for an autonomous vehicle based on an iot gateway and deep learning. Appl Sci 8:1164. https://doi.org/10.3390/app8071164
3. Yaqoob I, Khan LU, Kazmi SMA, Imran M, Guizani N, Hong CS (2020) Autonomous driving cars in smart cities: recent advances, requirements, and challenges. IEEE Network 34(1):174–181. https://doi.org/10.1109/MNET.2019.1900120
4. van Wyk F, Wang Y, Khojandi A, Masoud N (2020) Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans Intell Transp Syst 21(3):1264–1276. https://doi.org/10.1109/TITS.2019.2906038
5. Shen X, Fantacci R, Chen S (2020) Internet of vehicles [scanning the issue]. Proc IEEE 108(2):242–245. https://doi.org/10.1109/JPROC.2020.2964107
6. Alguliyev R, Imamverdiyev Y, Sukhostat L (2018) Cyber-physical systems and their security issues. Comput Ind 100:212–223
7. Alshdadi AA (2021) Cyber-physical system with IoT-based smart vehicles. Soft Comput 25:12261–12273. https://doi.org/10.1007/s00500-021-05908-w
8. Zaabi AOA, Yeun CY, Damiani E. "Autonomous vehicle security: conceptual model," 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), Seogwipo, Korea (South), 2019, 1-5, https://doi.org/10.1109/ITEC-AP.2019.8903691.
9. Steve Corrigan HP (2002) Introduction to the controller area network (CAN). Application Report SLOA101 1–7. http://www.rpi.edu/dept/ecse/mps/sloa101.pdf
10. Jeong Y, Son S, Jeong E, Lee B (2018) A design of a lightweight in-vehicle edge gateway for the self-diagnosis of an autonomous vehicle. Appl Sci 8:1594. https://doi.org/10.3390/app8091594
11. Zhou, Li, and Shen, "Anomaly Detection of CAN bus messages using a deep neural network for Autonomous Vehicles," Applied Sciences, vol. 9, no. 15, p. 3174, 2019
12. Chattopadhyay A, Lam K-Y, Security of autonomous vehicle as a cyber-physical system, (2017) 7th international symposium on embedded computing and system design (ISED). Durgapur, India 2017:1–6. https://doi.org/10.1109/ISED.2017.8303906
13. Intel Corporation, "Intel Automotive Security Research Workshops," [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ [Accessed on Feb 10, 2022]
14. Cui J, Lin SL, Giedre S, Fengjun Z (2019) A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Networks. 90:101823
15. Karl W, Taghi KM, DingDing W (2016) A survey of transfer learning. J Big Data 3(9):1–40
16. MathWorks, "Get Started with CAN Communication in Simulink," MathWorks, [Online]. Available: https://www.mathworks.com/help/vnt/ug/get-started-with-can-communication-in-simulink.html. [Accessed 9 9 2022]
17. MathWorks, "Adaptive Cruise Control System Using Model Predictive Control," MathWorks, 2022. [Online]. Available: https://www.mathworks.com/help/mpc/ug/adaptive-cruise-control-using-model-predictive-controller.html
18. Al-Haija QA, Smadi MA, Zein-Sabatto S (2020) Multi-class weather classification using resnet-18 CNN for autonomous IOT and CPS applications. Int Confer Computat Scie Computat Intellig (CSCI) 2020:1586–1591. https://doi.org/10.1109/CSCI51800.2020.00293
19. AlOmari AA, Smadi AA, Johnson BK, Feilat EA. Combined approach of LST-ANN for discrimination between transformer inrush current and internal fault. 2020 52nd North American Power Symposium (NAPS), Tempe, p 1–6. https://doi.org/10.1109/NAPS50074.2021.9449768
20. J. Qiu, X. Liang, S. Shetty, and D. Bowden, "Towards Secure and Smart Healthcare in Smart Cities Using Blockchain," 2018 IEEE International Smart Cities Conference (ISC2), 2018;1–4, https://doi.org/10.1109/ISC2.2018.8656914
21. Bizon N, Dascalescu L, Tabatabaei M, Naser. (2014) Autonomous vehicles: Intelligent transport systems and smart technologies. Mechanical Engineering Theory and Applications, Nova Science Publishers Inc, Series
22. Shi Y, Lv L, Yu H, Yu L, Zhang Z (2020) A center-rule-based neighborhood search algorithm for roadside units deployment in emergency scenarios. Mathematics 8:1734. https://doi.org/10.3390/math8101734
23. Ali Alheeti KM, McDonald-Maier K (2018) Intelligent intrusion detection in external communication systems for autonomous vehicles. Systems Scie Control Eng 6(1):48–56
24. Mahmoud O, Harrison O, Perperoglou AA et al (2014) A feature selection method for classification within functional genomics experiments based on the proportional overlapping score. BMC Bioinformatics 15:274. https://doi.org/10.1186/1471-2105-15-274
25. F. A. Fauzi, E. Mulyana, R. Mardiati, and A. Eko Setiawan, "Fuzzy Logic Control for Avoiding Static Obstacle in Autonomous Vehicle Robot," 2021 7th International Conference on Wireless and Telematics (ICWT), 2021. 1–5, https://doi.org/10.1109/ICWT52862.2021.9678436
26. Alsulami AA, Abu Al-Haija Q, Alqahtani A, Alsini R (2022) Symmetrical simulation scheme for anomaly detection in autonomous vehicles based on LSTM model. Symmetry 14:1450. https://doi.org/10.3390/sym14071450
27. Philipsen SG, Andersen B, Singh B (2021) Threats and Attacks to Modern Vehicles. IEEE Int Confer Inter Things Intellig System (IoTaIS) 2021:22–27. https://doi.org/10.1109/IoTaIS53735.2021.9628576
28. Negi N, Jelassi O, Clemencon S, Fischmeister S (2019) A LSTM approach to detection of autonomous vehicle hijacking. In: Proceedings of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems - VEHITS. SciTePress, p 475–482. https://doi.org/10.5220/0007726004750482
29. D. Kosmanos et al., "Intrusion Detection System for Platooning Connected Autonomous Vehicles," 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2019. 1–9, https://doi.org/10.1109/SEEDA-CECNSM.2019.8908528
30. Yang L, Moubayed A, Shami A (2022) MTH-IDS: a multitiered hybrid intrusion detection system for the internet of vehicles. IEEE Int Things J 9(1):616–632. https://doi.org/10.1109/JIOT.2021.3084796
31. Omar Minawi, Jason Whelan, Abdulaziz Almehmadi, and Khalil El-Khatib. 2020. Machine Learning-Based Intrusion Detection System for Controller Area Networks. In Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '20). Association for Computing Machinery, New York, NY, USA, 41–47. https://doi.org/10.1145/3416014.3424581

32. Alfardus A, Rawat DB, "Intrusion detection system for can bus in-vehicle network based on machine learning algorithms," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021. 0944-0949, https://doi.org/10.1109/UEMCON53757.2021.9666745.
33. Gad AR, Nashat AA, Barkat TM (2021) Intrusion detection system using machine learning for vehicular Ad Hoc networks based on ToN-IoT dataset. IEEE Access 9:142206–142217. https://doi.org/10.1109/ACCESS.2021.3120626
34. Abu Al-Haija, Q., Al Badawi, A., & Bojja, G. R. (2022). Boost-Defence for resilient IoT networks: A head-to-toe approach. Expert Systems, e12934. https://doi.org/10.1111/exsy.12934
35. Thaseen IS, Kumar CA (2017) Intrusion detection model using a fusion of chi-square feature selection and multi-class SVM. J King Saud University-Computer Inform Scie 29(4):462–472
36. Elreedy D, Atiya AF (2019) A comprehensive analysis of synthetic minority oversampling technique (SMOTE) for handling class imbalance. Inf Sci 505:32–64
37. Aloqaily M, Otoum S, Al Ridhawi I, Jararweh Y (2019) An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw 90:101842
38. Basavaraj D, Tayeb S (2022) Towards a lightweight intrusion detection framework for in-vehicle networks. J Sens Actuator Netw 11:6. https://doi.org/10.3390/jsan11010006
39. Yang F, Wang S, Li J, Liu Z, Sun Q (2014) An overview of the internet of vehicles. China Communicat 11(10):1–15. https://doi.org/10.1109/CC.2014.6969789
40. Abu Al-Haija Q, Zein-Sabatto S (2020) An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics 9:2152. https://doi.org/10.3390/electronics9122152
41. Zhang L, Ma D (2022) A hybrid approach toward efficient and accurate intrusion detection for in-vehicle networks. IEEE Access 10:10852–10866. https://doi.org/10.1109/ACCESS.2022.3145007
42. Purohit S, Govindarasu M (2022) ML-based anomaly detection for intra-vehicular CAN-bus networks. IEEE Int Conference Cyber Secu Resilie (CSR) 2022:233–238. https://doi.org/10.1109/CSR54599.2022.9850292
43. Ibrahim RF, Abu Al-Haija Q, Ahmad A (2022) DDoS attack prevention for internet of thing devices using Ethereum Blockchain technology. Sensors 22:6806. https://doi.org/10.3390/s22186806
44. A. M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, 1–8, https://doi.org/10.1109/ic-ETITE47903.2020.332
45. Liu H et al (2021) Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. IEEE Trans Veh Technol 70(6):6073–6084. https://doi.org/10.1109/TVT.2021.3076780
46. KDD Cup 1999 Dataset. The Fifth International Conference on Knowledge Discovery and Data Mining. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
47. Al-Haija QA, Alsulami AA (2021) High performance classification model to identify ransomware payments for heterogeneous bitcoin networks. Electronics 10:2113. https://doi.org/10.3390/electronics10172113the
48. Abu Al-Haija Q, Al-Badawi A (2022) Attack-aware iot network traffic routing leveraging ensemble learning. Sensors 22:241. https://doi.org/10.3390/s2201024
49. Durmanov A, Li M, Khafizov O, Maksumkhanova A, Kilicheva F, Jahongir R (2019) Simulation modeling, analysis and performance assessment. 2019 International Conference on Information Science and Communications Technologies (ICISCT). Tashkent, p 1–5. https://doi.org/10.1109/ICISCT47635.2019.9011977
50. Law AM. How to build valid and credible simulation models. In2019 Winter Simulation Conference (WSC) 2019 1402–1414. IEEE
51. K. Brett, Convolutional Neural Networks with Swift for Tensorflow: Image Recognition and Dataset Categorization., Jefferson, MO, USA: Apress, 2021
52. Muhammad TS, Muhammad ZA, Ahmad A, Adnan YSS, Ateeq UR (2022) Exploiting pre-trained CNN models for the development of an EEG-based robust BCI framework. Comput Biol Medicine 143:1–14
53. MathWorks, "Math. Graphics. Programming," MathWorks, [Online]. Available: https://www.mathworks.com/products/matlab.html. [Accessed on Mar 21, 2022]
54. Zijiang Z, Zhenlong H, Weihuang D, Hang C, Zhihan L (2022) Deep learning for autonomous vehicle and pedestrian interaction safety. Saf Sci 145:105479
55. Al-Haija, Q.A.; Gharaibeh, M.; Odeh, A. Detection in Adverse Weather Conditions for Autonomous Vehicles via Deep Learning. AI 2022, 3, 303–317. https://doi.org/10.3390/ai3020019
56. Nuha A, Khattab MAA (2020) Salah SAR "Intelligent intrusion detection system in internal communication systems for driverless cars." Webology 17(2):376–393
57. Abdallah GR, Ahmed N, Tamer MAB (2021) intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. IEEE Access 14(1):37–52
58. Seonghoon J, Boosun J, Boheung C, HuyKang K (2021) Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks. Vehicular Communicat 29:100338
59. Francesco P, Ennio AA, Simone C, Emanuele S (2021) Cybersecurity in automotive: an intrusion detection system in connected vehicles. Electro 10(15):1765
60. Yang L, Shami A (2022) A transfer learning and optimized CNN based intrusion detection system for internet of vehicles. ICC 2022 - IEEE International Conference on Communications. Seoul, Korea, p 2774–2779. https://doi.org/10.1109/ICC45855.2022.9838780
61. Liu Y et al (2023) Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises. IEEE Trans Industr Inf 19(1):635–643. https://doi.org/10.1109/TII.2022.3200067
62. S. Anbalagan, G. Raja, S. Gurumoorthy, R. D. Suresh and K. Dev, "IIDS: Intelligent Intrusion Detection System for Sustainable Development in Autonomous Vehicles," in IEEE Transactions on Intelligent Transportation Systems, https://doi.org/10.1109/TITS.2023.3271768
63. Song HM, Woo J, Kim HK (2020) In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications 21:100198
64. E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018 1–6, https://doi.org/10.1109/PST.2018.8514157
65. Cheng P, Xu K, Li S, Han M (2022) TCAN-IDS: intrusion detection system for internet of vehicle using temporal convolutional attention network. Symmetry 14:310. https://doi.org/10.3390/sym14020310
66. Cheng P, Han M, Li A, Zhang F (2022) STC-IDS: Spatial–temporal correlation feature analyzing based intrusion detection system for intelligent connected vehicles. Int J Intell Syst 37:9532–9561. https://doi.org/10.1002/int.23012

Publisher's Note