scientific reports

Check for updates

OPEN

An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks

Shanthalakshmi M ✉ & Ponmagal R S ✉

Smart cities have developed advanced technology that improves people's lives. A collaboration of smart cities with autonomous vehicles shows the development towards a more advanced future. Cyber-physical system (CPS) are used blend the cyber and physical world, combined with electronic and mechanical systems, Autonomous vehicles (AVs) provide an ideal model of CPS. The integration of 6G technology with Autonomous Vehicles (AVs) marks a significant advancement in Intelligent Transportation Systems (ITS), offering enhanced self-sufficiency, intelligence, and effectiveness. Autonomous vehicles rely on a complex network of sensors, cameras, and software to operate. A cyber-attack could interfere with these systems, leading to accidents, injuries, or fatalities. Autonomous vehicles are often connected to broader transportation networks and infrastructure. A successful cyber-attack could disrupt not only individual vehicles but also public transportation systems, causing widespread chaos and economic damage. Autonomous vehicles communicate with other vehicles (V2V) and infrastructure (V2I) for safe and efficient operation. If these communication channels are compromised, it could lead to collisions, traffic jams, or other dangerous situations. So we present a novel approach to mitigating these security risks by leveraging pre-trained Convolutional Neural Network (CNN) models for dynamic cyber-attack detection within the cyber-physical systems (CPS) framework of AVs. The proposed Intelligent Intrusion Detection System (IIDS) employs a combination of advanced learning techniques, including Data Fusion, One-Class Support Vector Machine, Random Forest, and k-Nearest Neighbor, to improve detection accuracy. The study demonstrates that the EfficientNet model achieves superior performance with an accuracy of up to 99.97%, highlighting its potential to significantly enhance the security of AV networks. This research contributes to the development of intelligent cyber-security models that align with 6G standards, ultimately supporting the safe and efficient integration of AVs into smart cities.

Keywords Transfer learning (TL), Intrusion detection system (IDS), Autonomous Vehicles (AV), Cyber-physical system (CPS), Controller area network (CAN)

Abbreviations

CPS	Cyber-physical system
AV	Autonomous vehicles
ConvNet, CNN	Convolutional neural networks
CAN	Controller area network
IIDS	Intelligent intrusion detection system
TL	Transfer learning
IDS	Intrusion detection system
ITS	Intelligent transportation systems
IoE	Internet of everything

Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, Tamil Nadu, India. ✉email: mshanthi.s@gmail.com; ponmagas@srmist.edu.in

IoT	Internet of things
SAGUN	Space air ground underwater network
AI	Artificial intelligence
ML	Machine learning
VANET	Vehicular ad-hoc network
DoS	Denial of services
MLP	Multilayer perceptron
FDI	False Data insertion
CDC	Cyber attack dataset collection
LSTM	Long-term short term memory
IDM	Intrusion detection mechanism
ACC	Adaptive cruise control

The rapid progress of 6G technology holds the potential to improve Intelligent Transportation Systems (ITS) making them more self-sufficient, smart and effective. Traditional ITS technologies have been widely adopted globally leading to enhancements, in vehicle capabilities. The economy's rapid expansion and urbanization's speed up have resulted in an increase in car ownership. By connecting transportation tools to traffic assets, Intelligent Transportation Systems (ITS) are a promising solution for traffic control that addresses the needs of linking people with other services[3].

Today, with the advent of urbanization, there is an increasing demand for intelligent ITS systems that can tackle problems like gridlock, boost traffic movement, minimize accidents and reduce energy usage and environmental pollution.6G will outdo personalized communications through full integration of the Internet of Everything (IoE) concept which connects people, vehicles, computing resources, wearable and sensors devices even robotic entities among others[36]. These challenges encompass resource management, privacy protection, security issues, learning and communication difficulties, standardized protocols, and the deployment of machine learning capabilities on IoT sensors[46].

The Space Air Ground Underwater Network (SAGUN) is expected to form the main architecture for the upcoming 6G network so as to facilitate fast and seamless connectivity[24,25]. Apart from improving communication metrics other researchers consider Artificial Intelligence (AI) as shaping 6G too. Advanced machine learning technologies are viewed as good tools for addressing complex challenges effectively[26,51].

Modern sensors, computation and network technologies come together in a cyber-physical system (CPS) to blend the cyber and physical world. On the other hand, if combined with electronic and mechanical systems, autonomous vehicles (AVs) provide an ideal model of CPS. AV components can be connected through sensors, ECUs and actuators in various vehicle network systems. Some common examples of such network systems are: FlexRay, Local Interconnect Networks (LIN) Controller Area Networks (CAN) and Time-Triggered CAN (TTCAN).

More research presents a layer-based classification of cyberattacks, grading them by integrity, availability, confidentiality, and accountability. It emphasizes the need for new approaches to address security issues in smart grids without reducing efficiency[45]. Addressing these speed and security issues through effective regulations and best practices is essential for safe and efficient integration into urban environments[47,56].

The development of internet-based smart appliances is a result of remarkable advancements in IoT as well as embedded systems. This has seen traditional cars transformed into "smart" fully functional machines that offer convenience while in transit. The ground-breaking features and possibilities provided by modern technology are the foundation for intelligent vehicles. Daily affairs have necessitated people to purchase these intelligent cars because they value comfort and safety above all else[35]. They possess attributes such as eco-friendly consciousness, online capability, and adherence to traffic provisions, self-piloting capacity, rapid decision-making abilities, passenger and pedestrian safety including parking among others. These autonomous vehicles are popularly known as driverless cars and mark the peak of smart vehicle inventions today. Autonomous driving is being considered the next disruptive innovation. Among image processing techniques involving neural networks, convolutional neural networks (CNNs) have been used because of their high performance in extracting information from images using convolution. Process 2D inputs through several layers for extraction of complicated features and find out useful patterns on a picture based on how pixels are arranged spatially. No preprocessing is required for CNNs since they are simple to implement.

The advantages to integrating ML throughout the network, there are still security issues, mostly with regard to authentication and data integrity. Notwithstanding its drawbacks, machine learning (ML) exhibits potential in domains such as personal identification and health data analysis; however, confidentiality and vulnerability management are critical[48]. To enhance IDS, researchers incorporated a feature selection and classification mechanism, which prioritizes essential information by removing unnecessary attributes from datasets[8]. Through their study, the researchers found that Decision Trees were the most effective ML technique for defending AVs against IDS attacks due to their reliability and consistency. This highlights the importance of using appropriate ML algorithms to enhance IDS performance in identifying and mitigating cyber-attacks in AVs.

Figure 1 represents the design of autonomous vehicle system. We can deploy VANET to meet your needs by accessing resources and connecting to the Internet while on the move. Additionally, other potential applications in health and safety, intelligent transportation systems, military systems, etc. were also expected. VANET allows you to group vehicles based on route, mobility, and on-road behavior, allowing you to maintain an adaptive approach to traffic monitoring and pollution density. The AV also uses this information to make adaptive decisions regarding route selection. Once the government approves vehicle-to-vehicle communication and all

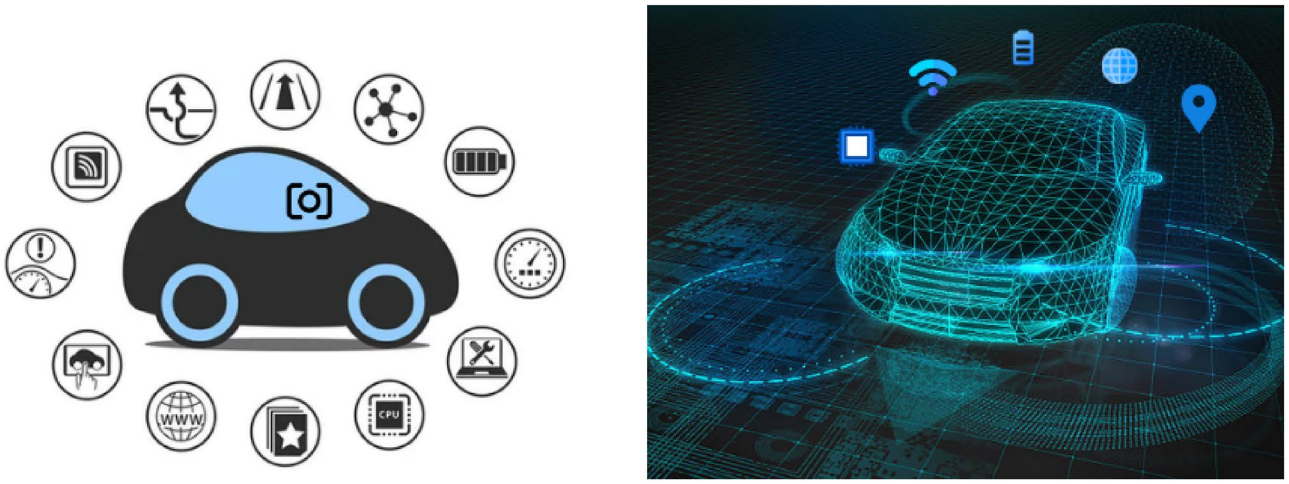

Fig. 1. Autonomous vehicle design.

cars adapt to it, it will become clear why it is so important to use VANET for tracking, navigation, routing or communication.

Generation	History	Advantages	Disadvantages
1G (Analog)	Late 1970s—Early 1980s	Pioneered mobile wireless communication Enabled widespread adoption of mobile phones	Poor voice quality and security Limited capacity and coverage High susceptibility to interference and eavesdropping
2G (Digital)	Early 1990s	Improved voice quality and capacity Introduction of SMS and basic data services Enhanced security and encryption	Limited data transmission rates Early 2G networks had slow data services compared to later generations
3G (Mobile broadband)	Early 2000s	High-speed data transmission, supporting video calls and mobile internet Enhanced capacity and coverage Support for a wide range of multimedia services	Higher costs for network deployment and maintenance Power consumption concerns for mobile devices
4G (High-speed mobile internet)	Late 2000s	Significantly higher data rates and capacity Improved spectral efficiency Support for HD video streaming, VoIP, and enhanced gaming experiences	Expensive infrastructure upgrades Potential for network congestion with increased data usage Battery life concerns for mobile devices
5G (Ultra-Fast, Low latency)	Late 2010s	Extremely high data rates and low latency Enhanced capacity for IoT devices and smart cities Support for autonomous vehicles and advanced industrial applications	High deployment costs and complexity Limited initial coverage, especially in rural areas Potential health concerns over higher frequency bands
6G (Future vision)	Expected around 2030	Projected to offer even higher data rates, ultra-low latency, and greater reliability Integration of AI for network optimization and autonomous operations Enhanced support for holographic communications and advanced VR/AR applications	Anticipated high costs for development and deployment Potential challenges in spectrum allocation and management Privacy and security concerns with highly connected environments

Objectives and motivation

In this work, we emphasize that all adopted regulations influence the vulnerabilities of devices used in AV, and these are directly linked to the intelligence level of the vehicle. Additionally, operational regulations with practical restrictions should govern the features of these AV devices. Motivated by these considerations, our objectives include: improving the reliability of the devices to prevent unnecessary vulnerabilities; safeguarding the services of all devices integrated into AVs; and developing an intelligent cybersecurity model that influences the policies adopted for AVs and their devices.

The widespread adoption of AVs has driven the development of numerous internal and external devices, such as sensors. As the number of 6G users increases, so does the connectivity, mobility, and vulnerability of the devices integrated into AVs. This leads to more interactions and a higher volume of unsecured communications. This research aims to mitigate these issues, including the associated costs and overall energy consumption. A system becomes vulnerable and a target for hackers when accurate policies are not provided promptly, leaving the system defenseless. It is crucial for the intelligent decision-makers within these systems to deliver policies promptly; otherwise, services, such as those of banks, will be susceptible to attacks. Timely delivery means considering all aspects, including clients, servers, and all interface links and communications.

Major contribution of the proposed work

In our proposed approach, we utilized policies derived from 6G guidelines. Intelligent cyber-security aims to enhance the cyber-security solutions of AV services by implementing policies based on 6G requirements and intelligence levels, which are directly related to the robustness of the policies. As the strength of the policies increases, the intelligence level in intelligent cyber-security solutions also rises.

This paper makes the following contributions:

Development of a technique that utilizes ConvNet (CNN) models to detect cyber-attacks on the interlinked components of AVs via the Controller Area Network (CAN).
Addressing the vulnerabilities of the CAN communication protocol within 6G vehicle networks, highlighting its lack of encryption and authentication, which poses risks to network security and the safety of individuals.
Utilization of pre-trained CNN models for the detection of cyber-attacks based on the Interactions and Interdependent Data Structures (IIDS) mechanism.
Creation of the IIDS mechanism, which enhances cyber-attack detection capabilities and Integration of Multiple Learning Techniques: Employment of four distinct learning techniques within the IIDS mechanism: Data Fusion, One-Class Support Vector Machine, Random Forest, and k-Nearest Neighbor.

The following topics are addressed later in this paper. Sect. "Related work" discusses the various research studies conducted recently and the available approaches of detecting CPS cyber-attacks. The discussion about the proposed solution with the implementation of AV-CPS is in sect. "Methodology". Its efficiency has been determined through result analysis contained in sect. "Experimentation and result discussion", while it has been proved to be more accurate than any usual approach suggested in sect. "Experimentation and result discussion". In sect. "Conclusion", conclusion is given.

Related work

Smart cities and their applications and services are at a higher development pace due to the rapid advances in artificial intelligence, communications, and remote sensing. To enhance living standards of smart cities, various smart services in such areas as communications, cyber security, smart grids, healthcare, and transportation systems are emerging and being industrialized. The main attention was focused on intelligent mobility and intelligent transportation systems that include autonomous cars. It is predicted that within a few years more than 300 million AV's will be connected to roadside units. Nevertheless, despite the tremendous growth of the industry of self-driving cars these vehicles still remain susceptible to multiple cyber-attacks with consequences ranging from minor disruptions to severe threats against life and health of individuals[2]. There is a broad scope for possibilities. Therefore multiple researches have been done on this issue as well as numerous systems created to study, recognize and diminish cyber-attacks or threats occurring in the autonomous vehicle system Most of these studies integrate diverse machine learning (ML) techniques with cyber security measures to build security and defense systems for them.

In this regard, it will be significant to note that a new intelligent intrusion detection method has been proposed towards safeguarding autonomous vehicle's external communications[9]. This mechanism exploits a blend of hybrid intelligent intrusion system comprising overlapping criteria proportional score (POS) techniques, multilayer perceptron (MLPs), and fuzzy sets that detect activity in connected and communicating self-driving cars[11]. To spot denial of service attacks (DoS), we apply the hybrid IDS back propagation neural network. Experimental evaluation results have shown that this detection system is very effective in identifying DoS attacks in autonomous vehicles. However, these models are related with increased interpretation costs because of computational processing by different sub-systems such as pre-processing sub-system, feature extraction sub-system with POS module and fuzzification sub-system. They have given a technique to detect wrong insertion of data in self-driven cars[19–21].

Guo et al.[57] proposed a two-tiered security framework. The first component is a reinforcement learning model designed to evaluate message credibility. To enhance the accuracy of these evaluations, a context-aware trust management model is introduced. This second component selects the most appropriate evaluation method, thereby improving the overall precision of the framework[57].

This is where he has his three subsystems. False Data Insertion (FDI) Subsystem imitates attacks on self-driving cars. The Cyber Attack Dataset Collection (CDC) Subsystem. Normal and attack mode simulation models for creating and collecting of data[23]. A deep long-term short term memory (LSTM) network is used by the Intrusion Detection Mechanism (IDM) Subsystem to detect types of cyber-attacks such as FDI attacks on vehicle control systems [30]. The system labels data samples as normal or abnormal. Results from their experimental evaluation show that their model worked well with high detection rates compared to other state-of-the-art methods[33,39]. However, their proposed system was only tested against simulated data sets without incorporating any control communication system in the self-driven car.

The authors of[49] developed a novel auto encoder-based detection framework for identifying attacks in Industrial IoT (IIoT) networks, utilizing Recurrent Neural Networks (LSTM) and Convolutional Neural Networks (CNN). The key advantage of this framework is its ability to detect both novel (zero-day) and conventional IIoT attacks by combining LSTM and CNN[54]. Additionally, each prediction made by the CNN-LSTM model is accompanied by a local explanation using the LIME technique. Similarly, Khan et al.[50] introduced an unsupervised anomaly detection system aimed at identifying IP-based attacks such as denial-of-service (DoS), reconnaissance, exploits, fuzzes, and generic attacks. The system operates in two phases. The first phase employs two models based on the conventional state-based approach, while the second phase utilizes a bidirectional LSTM-based technique[53]. These models were implemented at the gateway of the connected vehicle. The system

was evaluated using the UNSW-NB15 dataset, and its effectiveness was measured using accuracy, recall, precision, and F1-score.

Smart transportation systems, particularly those reliant on autonomous vehicles, face significant security and privacy risks. Despite their potential to improve traffic flow, safety, and environmental impact, these complex systems are vulnerable to cyber- attacks. To address these challenges, innovative network structures like Space-Air-Ground Integrated Vehicular Networks (SAGIVNs) are being explored. However, even these advanced systems require robust security measures to protect against threats that could compromise user privacy and system integrity. Ultimately, the successful implementation of smart transportation hinges on developing effective solutions that safeguard both privacy and security[52].

Smart transportation systems, particularly those involving AVs, face significant cyber physical risks. The increasing reliance on interconnected devices (IoT) creates vulnerabilities similar to those seen in other sectors like utilities and manufacturing. Protecting these systems requires a comprehensive approach beyond traditional digital security. The complex interplay of digital and physical components in these systems demands new security measures. Existing digital security practices are insufficient to protect against the evolving threats in this domain.

Essentially, the integration of numerous sensors and actuators in autonomous vehicles, while enabling advanced features, also creates a larger attack surface. To safeguard these systems, a holistic security strategy is crucial, considering both digital and physical vulnerabilities.

Methodology

In smart cities, Autonomous Vehicles (AVs) are a typical example of how Cyber-Physical Systems (CPS) principles work and they raise the standards of urban life through curbing energy consumption and air pollution. For instance, cloud computing is very important in AV-CPS especially when it comes to IT integration and communication processes which should be scalable for real-time data processing, analysis and storage as well as promoting smooth operation of such systems in smart urban areas. Moreover, AVs are prone to cyber-attacks such as key fob cloning, telematics service disruptions radar interference sensor spoofing ultrasonic sensor tampering camera sensor attacks lidar sensor interference etcetera including emergent threats e.g. ransomware vehicle theft among others. As a result, this article proposes a technique that employs pre-trained ConvNet models to expose the cyberattacks targeted at the interlinked mechanical components of motor vehicles using the CAN communication protocol.

Simulation of AV systems

Simulation is a computerized model used for assessing the performance of a prototype before it moves to production. Using simulation models rather than physical models has several advantages including cost effectiveness, ease of implementation, testing and maintenance. The self-driving car system research employs a simulation model of an autonomous vehicle system which consists of front vehicle and self-propelled vehicle (self-driving car). The self-propelled vehicle should at all times maintain its distance from the front vehicle using the ACC under perfect conditions. Hence, it is necessary for the two-wheeler on the rear side to keep constant track of where its leading counterpart is situated. In this case, we will focus on three important components that make up the self-propelled vehicle: Velocity sensor, position sensor and ACC as indicated in Fig. 2.The velocity

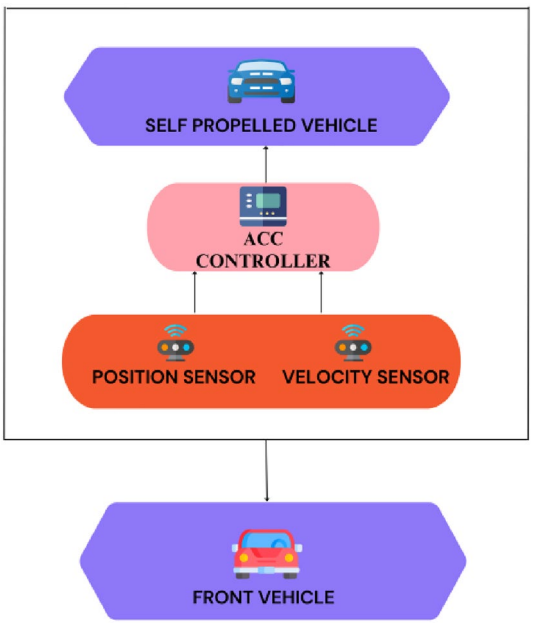

Fig. 2. Simulation of AV systems.

sensor is used to measure the speed while the position sensor detects how far away from both cars are from each other. ACC receives these readings and subsequently adjusts the speed so as to match that of the front car.

CAN communication network

To reduce the increasing number of wires in cars that hampered their reliability, Bosch developed CAN protocol in 1985. Although it processes only a limited amount of real-time sensor data, CAN is a standard communication protocol for managing vehicle control and sensor data[18]. Furthermore, to collect data flows from all major automotive core control systems: engine transmission body systems among others into CAN bus broadcasting each piece of information to the CAN bus. There is always an open network at any node that implies that any CAN network node in a vehicle can be attacked by harmful internal or external sources. As more sensing and communication equipment is required for independent operation of AVs, security risks increase with autonomy levels.

CAN Network serves as a utilized communication protocol in 6G vehicle networks; however its lack of encryption and authentication exposes vulnerabilities to attacks and misconduct, by vehicle users posing risks to network security and the safety of vehicle occupants. The most used communication protocol in 6G vehicle networks is CAN. This can make the network vulnerable to attacks and harmful acts by motorists that could put the lives of passengers at risk because it does not have encryption and authentication measures to protect against such events[10]. Consequently, there is a pressing need for better intrusion detection systems in 6G vehicular networks that allow the network to modify its environment in order to meet different application requirements and service types as fast as possible. Figure 3 represents CAN data transfer system.

The CAN bus acts as a broadcast system, allowing all nodes to receive all transmissions. It's not possible to target a message to a specific node; all nodes inevitably capture all traffic. However, the CAN hardware offers local filtering, enabling nodes to respond solely to pertinent messages[43]. CAN employ brief messages with a maximum payload of 94 bits. Messages do not contain explicit addresses; rather, they are content-addressed, meaning the content implicitly defines their destination.

Autonomous Vehicle—Cyber Physical Systems

Cyber-Physical Systems (CPS) combines computation, verbal exchange, and physical techniques, ranging from small-scale wearable clinical gadgets to massive-scale countrywide energy grids[15]. The middle concept of CPS is the seamless integration of cyber components and physical elements, with applications in car, avionics, robotics, healthcare, and energy grids[1]. CPS design historically separates manage set of rules concerns (handling bodily dynamics) from cyber implementation structures (data processing and networking).

Autonomous Vehicles (AVs), alternatively, are able to navigating and making choices without human input. They utilize sensors (like lidar, radar, and cameras), on-board computers, and control algorithms to sense their environment and make riding selections. AVs' levels of autonomy range from driver assistance structures (such as adaptive cruise manage) to finish autonomy (no human intervention)[4]. Figure 4 represents autonomous vehicle systems in collaboration with cyber physical systems.

Relationship between Autonomous Vehicles and Cyber-Physical Systems:

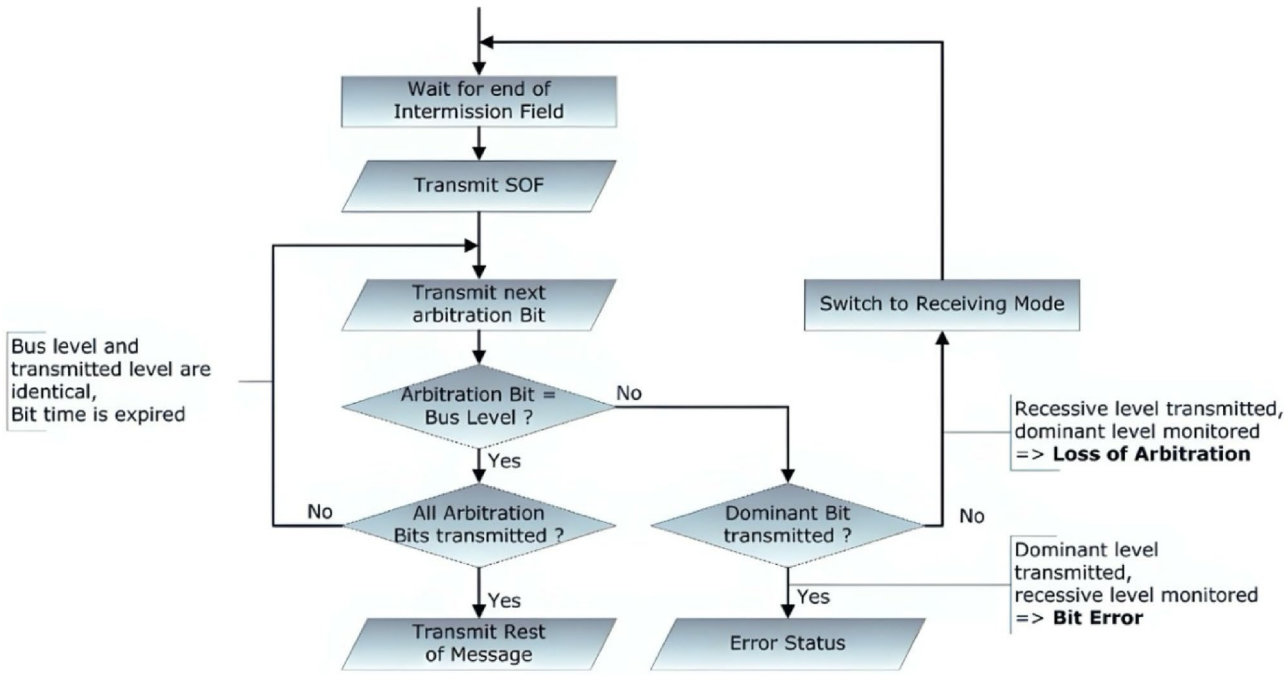

Fig. 3. CAN data transfer structure.

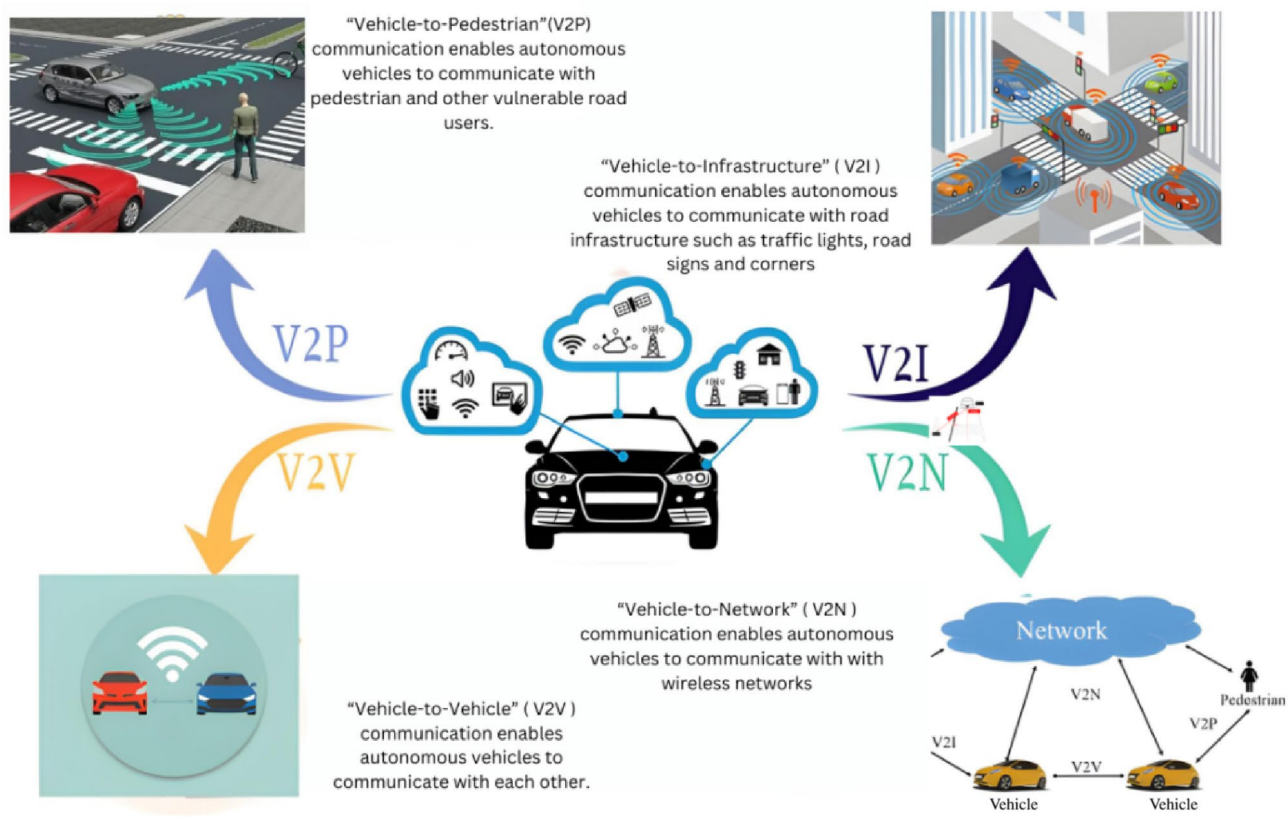

Fig. 4. AV in collaboration with CPS module.

1. Physical aspect:—AVs interact with the bodily global, such as roads, traffic, pedestrians, and weather conditions.—Their movements (steering, braking, and acceleration) have direct environmental effects.
2. Cyber aspect:—AVs rely upon cyber components:—Sensor Fusion: AVs integrate records from a couple of sensors (cyber) to form a entire environmental photograph (physical).—Control Algorithms: AVs employ manage algorithms (cyber) to handle physical dynamics (ex, lane upkeep, obstacle avoidance).—Communication Networks: AVs use wireless networks (cyber) to talk with different vehicles (V2V) and infrastructure (V2I).—Safety–Critical Systems: AVs' dependable and secure operation includes cyber additives.—Machine Learning: AVs follow system getting to know algorithms (cyber) to beautify belief.

The self-driving motorcar—cyber physical system is made up of the following subsystems: Sensors, actuators, two CAN nodes with names Node A and B and a controller. Nodes A&B communicates with each other through the signals as shown in Fig. 4 and the same is simulated with the activity of the CAN communication within the AV-CPS. Therefore, node A will get these signals.

- The current location of the self-propelled vehicle.
- The current position of the front vehicle
- The current speed of the self-propelled vehicle
- The current speed of the front vehicle
- The temporal interval
- The Target velocity

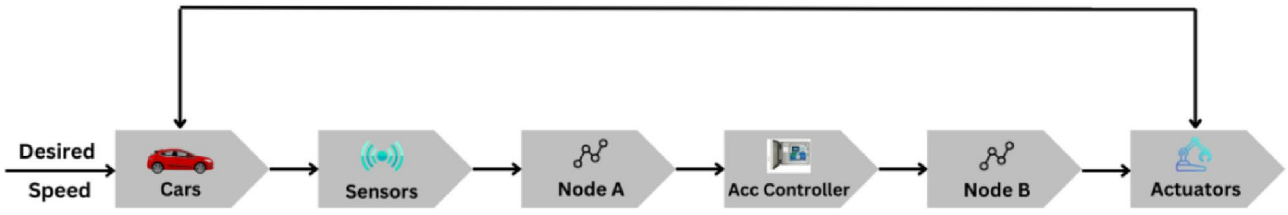

Fig. 5. Implementation of AV-CPS (self-propelled vehicle).

The position of the vehicle is measured in meters and velocity in m/s. The time interval between the car ahead and the self-propelled vehicle is 1.4 s. Next, the target speed is 30 m/s Upon receipt of such signals by ACC from Output, it will produce a control signal for adjusting the speed of self-propelled vehicle to meet up with a target velocity or front vehicle's position. In turn, nodes B send these commands to actuators which convert them into physical motion of the vehicle.

Dataset generation

Let us assume that the implementation of AV-CPS is done with various components like sensors,ACC controller,Node A,Node B,actuators as shown in Fig. 5. There is a possibility that an attacker may insert any malicious data through the attacked Node A which causes data spoofing/data tampering. The ACC received erroneous data regarding the self-propelled vehicle's position, leading to the generation of flawed control signals. Figure 5 represents the ordinary status of AV-CPS which has zero cyber-attack. Figure 6 depicts the scenario of the unusual condition wherein the attacker targets Node A. The raw dataset consists of one dimension and comprises 80,000 data points. The dataset is evenly balanced, with 40,000 data points labeled as normal and the remaining labeled as attack data. Basically, these four characteristics make up the dataset:

1. The current position of a self-propelled vehicle.
2. The present position of a front vehicle.
3. The speed at which the self-propelled vehicle is going at that particular time.
4. The rate at which the front vehicle is moving.

Intelligent Intrusion Detection Systems

Intrusion Detection Systems are systems that identify unauthorized access by hackers and malicious actors. These systems are usually implemented in places where frequent monitoring for any suspicious access to any secure data to ensure data integrity and security[7,22]. It checks for any behavioral anomalies and notifies the user about the malicious activity if found. This intelligent system is very promising when it is almost impossible to monitor an important system all the time, especially in the cases of monitoring in distant lands[16,17].

IIDS in Autonomous Vehicles

For self-using cars, there may be a want for coordinated Intrusion Detection Systems (IDS). These structures are incorporated into the automobile`s state-of-the-art structure to check and examine facts flows, perceive any uncommon structures or capability protection dangers and observe non-stop data and gadget mastering strategies to quick perceive unique functions in actual time, permitting quicker responses to cyber threats and unauthorized tries. The complexity and interconnectedness of superior automobile structures poses brilliant demanding situations for IDS in self-sustaining cars[5].

The complicated provisioning of sensors, manage structures, and network affords a huge spectrum of assaults that may be abused via way of means of malicious actors. A key undertaking is securing controller region management (CAN) communication, a important meeting in cars that calls for strong protection publicity to keep away from vulnerabilities[12].

The modern evolution of cyber threats poses a hazard to self-sustaining cars. These assaults goal flaws inside the gadget configuration, the communications network, or interference inside the outside drive, in all likelihood compromising its capability and protection data-pushed assaults, monitor quite a few demanding situations, and attackers manage facts to misdirect the gadget considering the calculations of self-sustaining cars, using to incorrect selections and sports.To keep away from getting self-sustaining cars need to be customer-centric facts safety comes first[13]. The IDS needs to paintings with actual-time vertical reaction to differentiate and save you from cyber threats, guard the application of the automobile and make certain occupant protection. Managing

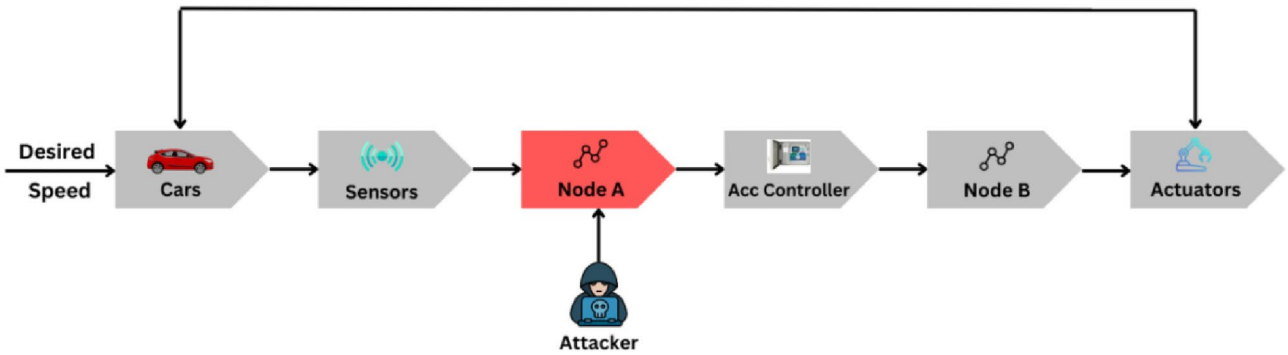

Fig. 6. Cyber attack in AV-CPS.

those demanding situations calls for a complete method that consists of a robust cyber security strategy, relentless checking out and refinement of protection platforms, collaboration with enterprise friends mounted cyber security suggestions for self-sustaining cars, and the continuing pursuit of systematic size to enhance IDS abilities towards superior cyber threat ranges can assist flow forward, that are intermediate operations that assure their protection.

As the technology develops rapidly, newer ML models are found and are used to improve the levels of Autonomous Vehicles. These new models ensure that IDS systems are more accurate to avoid any malicious attacks. Models like EfficientNet, DenseNet, InceptionV3, Inception ResNet V2, VGGNet, NasNet, and ResNet are some of the most powerful, current advanced ML models that are used in many autonomous vehicles.

ML with IIDS

Machine Learning and Intelligent Intrusion Detection are core building blocks of synthetic intelligence, both immediately concerned with data analysis, pattern reputation and selection making. ML is the sphere of look at granted for the development of structures that may analyze from statistics to discover samples and make predictions autonomously[31,32]. In contrast, IIDS is a complex record systems machine in which entities interact, even though forming complex relationships challenging to examine through traditional methods. The interplay between IIDS and ML algorithms enhances both my understanding and the functioning of such algorithms. In IIDS, Machine Mastery tech mainly performs well in data mining insights from the connectivity available in big datasets[34]. By applying to IIDS machine learning techniques like neural networks, decision trees or clustering that consist of graphs, relational databases and know-how graphs we can reveal hidden patterns, relationships or trends.

Integrating machine learning (ML) with intelligent and intrusion detection (IIDS) has several advantages like Analyzing structured data for complex relationships between entities. For example, nodes can be detected by using social network analysis based on ML. This can help you predict your network user's actions based on their interactions within it. ML applied to genetics can find relations between organic objects through genetic traits[40,41].

In addition to that, having partnership between ML and IIDS facilitates innovation in areas such as Natural language processing, Image recognition, Recommendation systems and Self-driving cars. Through these approach researchers working within these domains would use ML algorithms for processing his/her related data concerning IIDS helping him/her to enhance language models, increase accuracy while reflecting adjustments according to user preferences and improve the system's decision making ability[42].

Transfer Learning

Transfer learning in machine learning is also a technique that allows knowledge from one task to be used to achieve better results on another task. This entails reusing knowledge acquired from previous tasks so as to enhance efficiency and speed up the training of new tasks[14]. This comes in handy when there are insufficient labeled instances from target domain hence models can rely on their experience with other similar domains as expertise. Transfer learning involves several types such as instance-based transfer, parameter transfer, feature-representation transfer and relational-knowledge transfer, each one focusing on different aspects of transferring knowledge across domains. When there are minor dissimilarities between the two domains or limited labeled data available for the target domain, marginal distributions adaptation, learned structure transfer or weights reassignment is an effective way to optimize model performance through transfer learning. In neural network models that involve Transfer Learning, what occurs instead is using pertained representations of features in place of starting over again with a fresh model. By doing this, it is possible to solve problems associated with small datasets by learning from past experience and applying them in future related tasks through this approach[44].

Experimentation and result discussion

The experiment was carried out with the help of MATLAB and Simulink. MATLAB is a powerful programming approach used by programmers for the analysis and design of products and systems that can take technology to the next level, while Simulink is a graphical programming platform that works on a MATLAB model for modeling and simulating. The AV animation demonstration was devised by MathWorks making use of MATLAB and Simulink. This study carried out the CAN component assembly utilizing the Simulink organize tool kit, later programmed in the AV rest using MATLAB to accomplish and examine the pre-trained CNNs looked at.

We developed a preparation test system by implementing a digit system using a Design preparing unit (GPU) to minimize the processing duration, and optimize the execution of the test. To fix the input of the pre-trained neural structures, we need to convert 1-D information to 2-D information model. Figure 7 represents the conversion of 1D image to 2D image. In the first phase, AV-CPS interests are developed. Step 2 records the responses to the points as previously identified as statistical 1-dimensional information in a chart. At that point, step 3 changes the information leading it from a 1D grid to a 2D structure. Step 4 includes storing the 2D presentation as an image. Each image has a measurement area of 4×81. Since we got four points, our computation is 4×81, and the animation runs 81 s each time. In the end, stage 5 collects and saves the resultant normality and abnormality images in separate folders.

Algorithm 1 shows the algorithm that how the information in part 1 was converted into two parts. First, 'image index' will be initialized with 0. Then decide it can be reshaped or not. 'current_row' and 'end_row' factors are utilized as counters since we propose to integrate all four data set lines. Therefore, ordinary information and

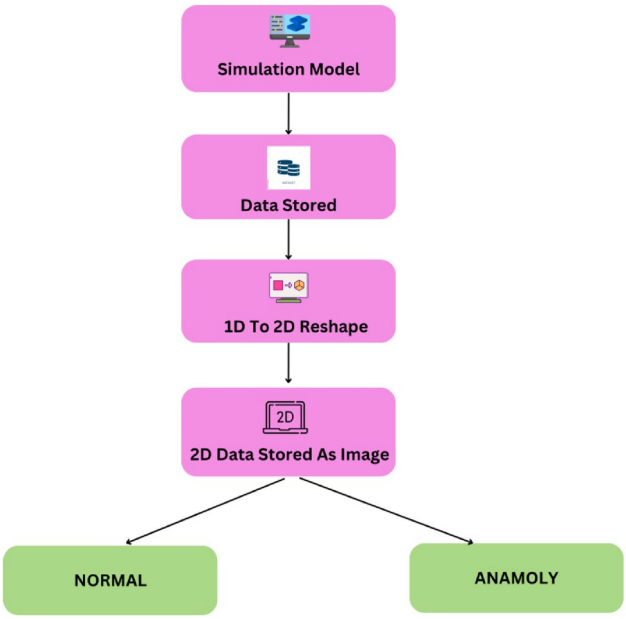

Fig. 7. Steps involved converting 1-D image to 2-D image.

attack information has been collected for use. The 'normal' catalog comprises images with specific information, and the 'attack' registry is designed to keep attack images. Where the circle begins with one and goes the length of the information source, whether specific or attack. So a few thousand copies are made of which halves of them were listed as ordinary and the rest as attack. Each image will be compressed in jpg format.

The following mentioned models are various current, powerful ML models used in Autonomous Vehicles along with their accuracies[6]. These have been billed as an integral part of sophisticated study paradigms in Intelligent Intrusion Detection in Autonomous Vehicles. Figure 8 illustrates the resizing of images for various models. EfficientNet, DenseNet, InceptionV3, InceptionResNet V2, VGG Net, NasNet, and ResNet 18 are published free of charge for their important parts in solving critical vehicle decision statistics[27,28]. Figure 9 represents the working model of intelligent intrusion detection system.

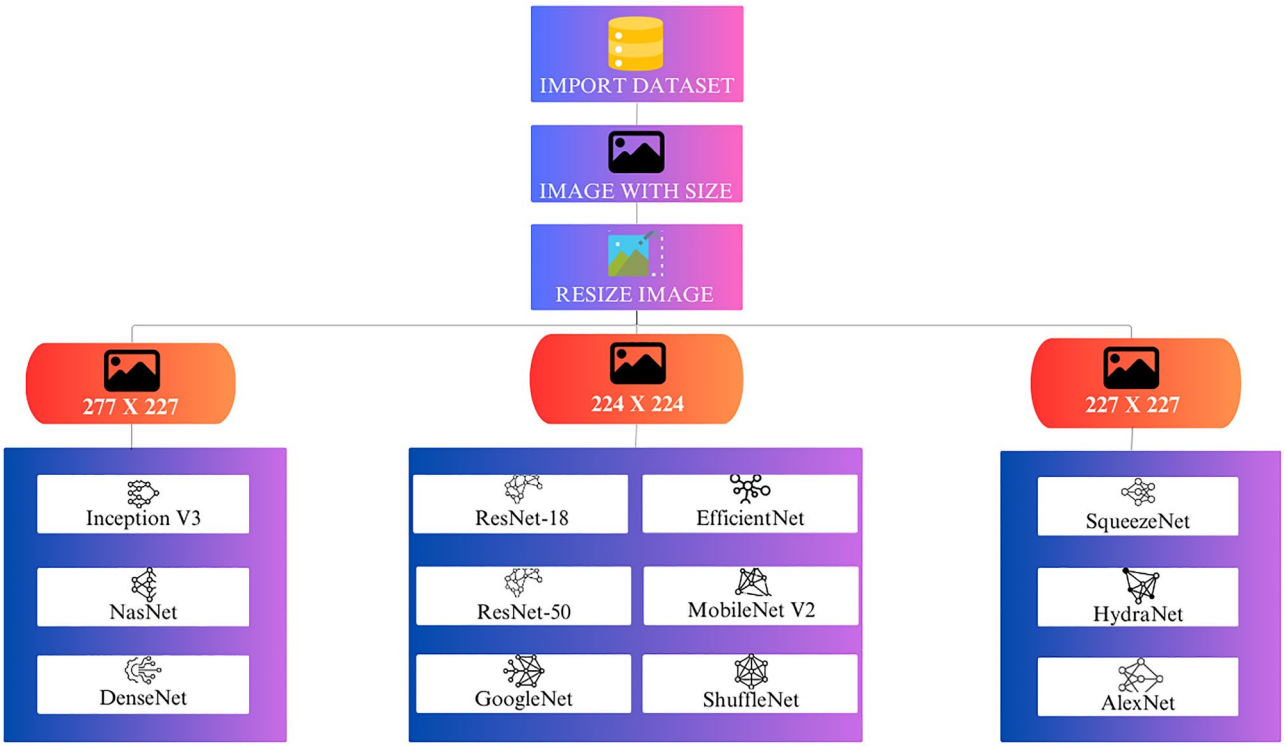

Fig. 8. Resizing of images for various models.

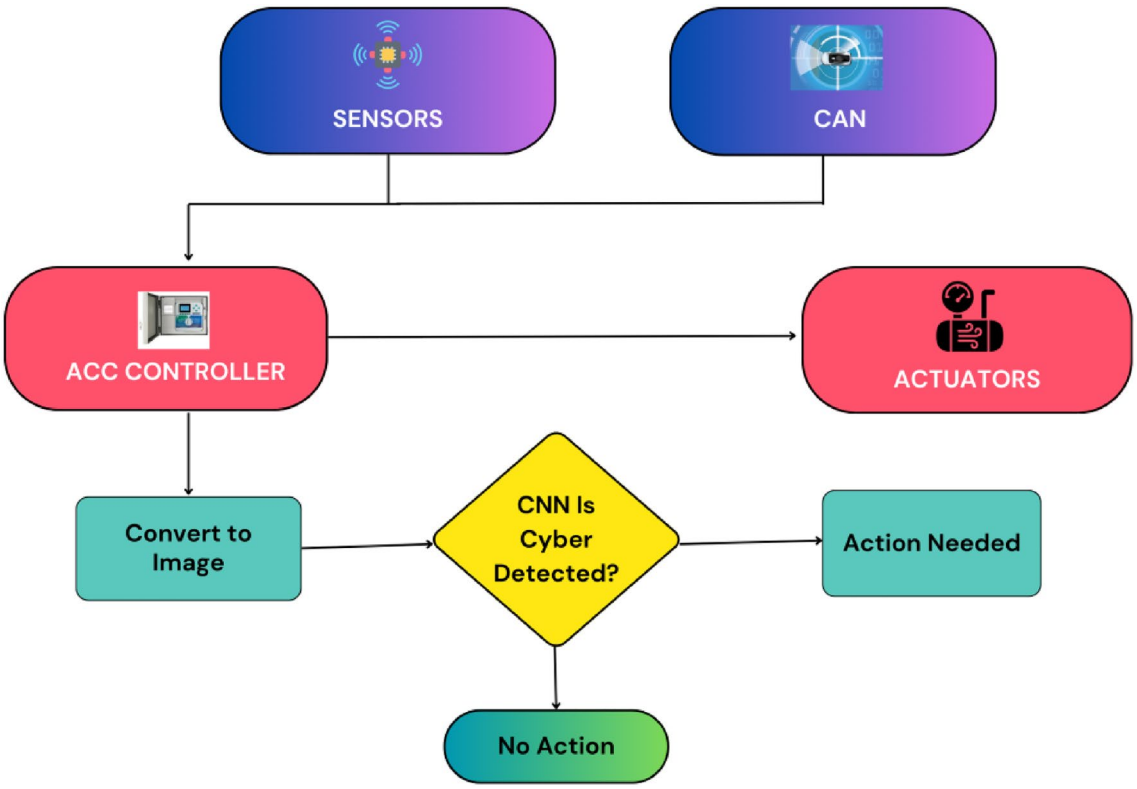

Fig. 9. Working principle of IIDS.

Input:

1. normal_data: Array of normal data
2. attack_data: Array of attack data
3. decision: String, either "normal" or "attack"

Output:

1. A series of JPG images saved in directories named "normal" or "attack"

Steps:

1. Initialization:
   - Initialize image_index to 0.
   - Initialize current_row to 1.
   - Initialize end_row to 4.
2. Data Loading:
   - Load the normal data.
   - Load the attack data.
3. Case Selection:
   - Set decision to either “normal” or “attack.”
4. Create Directory:
   - Create a directory named after decision if it does not exist.
5. Processing Data Subsets:
   - While current_row is less than or equal to the size of the selected data source:
     1. If decision is “normal”:
     - Set data_subset to a subset of normal data from index current_row to end_row.
     2. Else if decision is “attack”:
     - Set data_subset to a subset of attack data from index current_row to end_row.
     3. Reshape data_subset into a 4x8 array named image.
     4. Increment image_index by 1.
     5. Create a JPG image named image_index.jpg and store it in the folder corresponding to decision.
     6. Increment end_row by 4.
     7. Increment current_row by 4.
   - End Loop

Algorithm 1. To convert 1D image to 2D image.

The experiment was first started with two ML models ResNet—18 and NasNet[55]. After training and testing, their accuracy values were not up to the mark as they gave accuracy values of 97.65% and 98.18% respectively. Due to its susceptibility to over fitting, ResNet–18 provided lower accuracy, while due to its potential computational complexity and resource requirements, which may hinder its efficiency in real-time intrusion detection tasks, especially in dynamic and complex environments, NasNet provided lower accuracy. Hence we went for other advanced models namely ShuffleNet, MobileNet V2, and HydraNet. HydraNet is a strong ML model used in Tesla’s present models like Tesla Model 3, Tesla Model S, etc. The aforementioned models provided a good accuracy of 99.30, 99.30, 99.33% respectively. Even though they are significantly higher than the previous models, they are still very far from reaching a 100% accuracy rate[29,37].

The potential challenge in capturing complex and intricate patterns present in the data related to network intrusions in dynamic and evolving environments made ShuffleNet to provide lesser accuracy while the lightweight design of MobileNet V2 optimized for efficiency, may compromise its ability to capture and analyze complex and intricate patterns and HydraNet’s reliance on statistical trust-based methods and weak hidden Markov models made these models to provide lesser accuracy rate. This in turn made us move on with higher and more powerful models like GoogleNet, InceptionV3, DenseNet, and EfficientNet. Of those aforementioned ML models, GoogleNet is currently the strongest model with an astonishing accuracy rate of 99.47%. Even though it is almost close to being 100%, Inception V3’s 99.6%, DenseNet’s 99.8%, and EfficientNet’s excellent, mind-blowing 99.97% made it more clear that there exists many stronger models than present GoogleNet. For sure, we went for the best in the industry, EfficientNet. EfficientNet’s exceptional execution, with system accuracy of up to 99.97%, and DenseNet’s basic test accuracy of 99.8% highlight their plethora of basic techniques in fully classifying images and real-time data[38].

Metrics like Precision, Recall, F1-Score, and Accuracy are calculated using the formulae,

$$\text{Precision} = \frac{\text{TP}}{(\text{TP} + \text{FP}) * 100} \tag{1}$$

$$\text{Recall} = \frac{\text{TP}}{(\text{TP} + \text{FN}) * 100} \tag{2}$$

$$\text{F1} - \text{Score} = 2 * ((\text{Precision} * \text{Recall})/(\text{Precision} + \text{Recall})) * 100 \tag{3}$$

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN}) * 100} \tag{4}$$

where,

- TP—True positive.
- TN—True negative.
- FP—False positive.
- FN—False negative.

Confusion matrix can be used to find out the above mentioned terms. TP stands for true positive that represents the number of normal images classified correctly. FP refers to false positives that refer to normal images classified incorrectly. FN stands for false negative indicating normal images misclassified as abnormal ones. Finally, TN is called true negatives meaning there are abnormal images recognized correctly. Precision is a measure of how well the classifier separates positives from negatives which can be calculated using Eq. (1). Precision values for various models are represented in Fig. 9.Recall on the other hand can be determined by following Eq. (2). Recall values for several models are shown in Fig. 10.The F1 score combines precision and recall as in Eq. (3), whereas accuracy classification was determined using Eq. (4). Figures 11, 12 represent the F1 score and accuracy for various models accordingly. On comparison of various accuracy values provided by the aforementioned ML models, EfficientNet emerges as the best model with an incredible accuracy of up to 99.97%. Since the accuracy is almost close to 100%, this model is more promising in vehicles safety and protection against any malicious attacks. As shown in Fig. 13, this research also proves that EfficientNet – B7 works better than GoogleNet (accuracy—99%), which is currently the most powerful and secure model. Figure 14 represents a comparative analysis of the proposed model, EfficientNet-B7, with existing machine learning models. Figure 15 provides the training and validation loss & training and validation accuracy of ResNet-18 model. Figure 16 represents the training and validation loss & training and validation accuracy of ResNet-50. The training and validation loss & training and validation accuracy of AlexNet is represented in Fig. 17. Figure 18 provides the training and validation loss & training and validation accuracy of InceptionV3. The training and validation loss & training and validation accuracy of DenseNet is represented in Fig. 19. Figure 20 represents the training and validation loss & training and validation accuracy of proposed system—EfficientNet. From the analysis of these

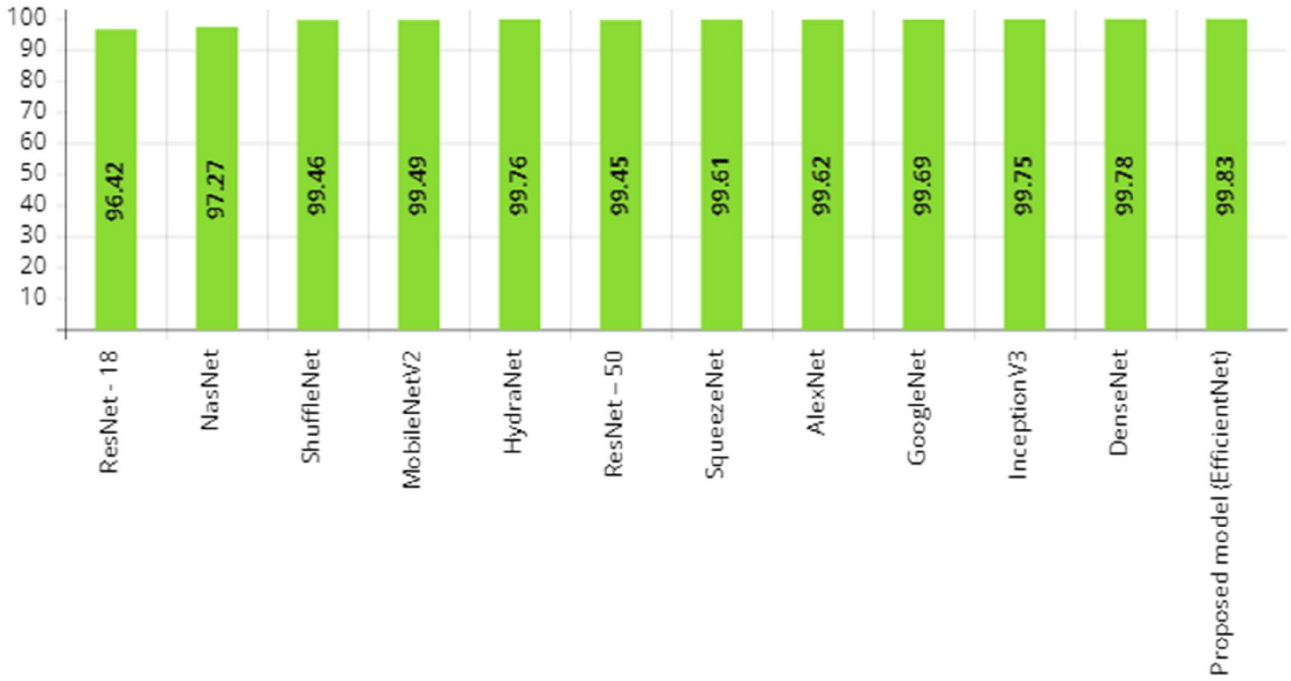

Fig. 10. Precision analysis.

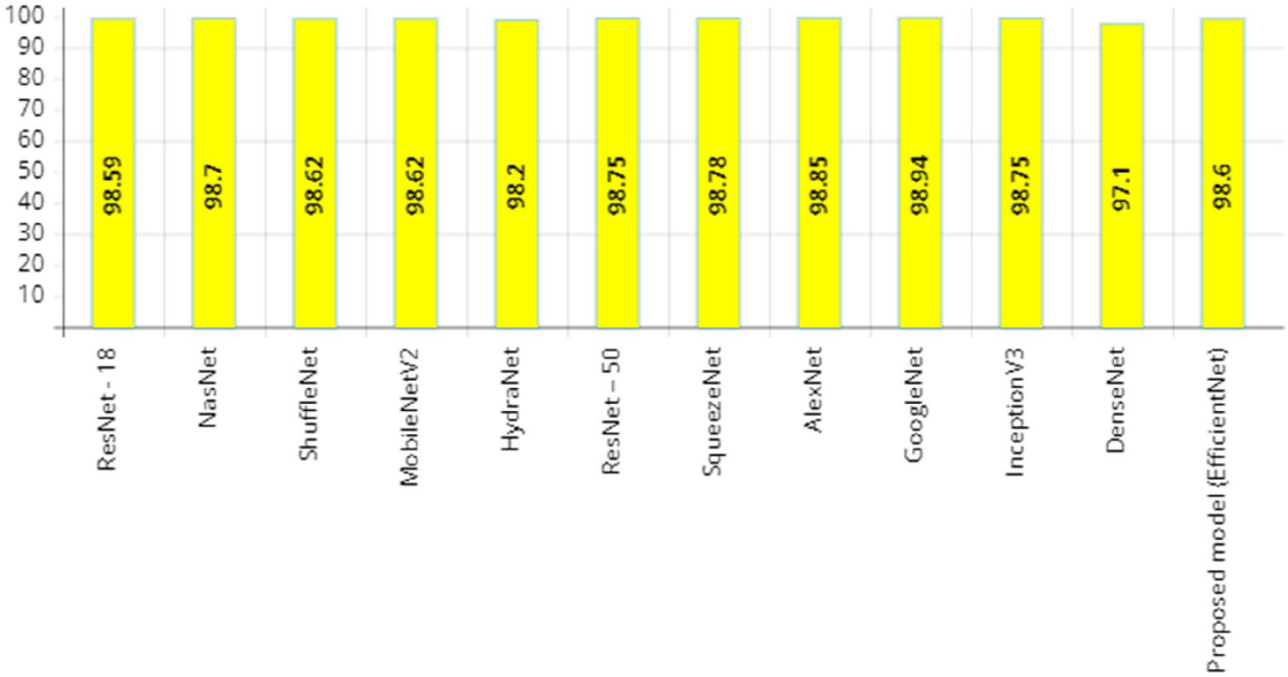

Fig. 11. Recall analysis.

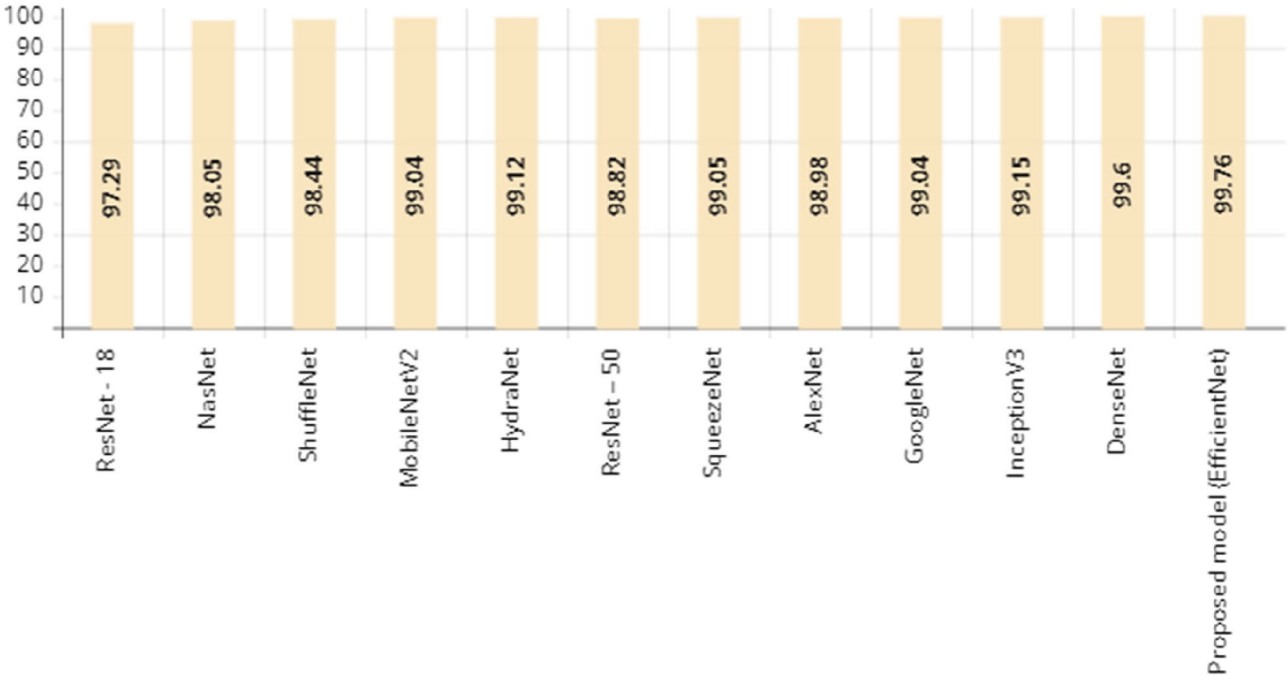

Fig. 12. F1 Score analysis.

graphs it is cleared that the proposed system has better accuracy when it is compared with the existing systems. The reason for the improvement is that the proposed system employs EfficientNet which provides the efficient classification thereby it improves learning in the network.

Looking at Table 1, we can see the calculation of the accuracy of pre-trained models that focuses on four metrics with regard to accuracy analysis. We compared the performance outcomes of this research with recent IDS methods employed in AV systems to validate and verify our work. The cost analysis of all models is provided in Table 1. Due to the complexity of the proposed EfficientNet model's architecture, it requires 12 GPU hours for computation. Despite its complexity, this model achieves higher accuracy compared to the other models, while also having a lower computation cost than the DenseNet model. Table 2 gives details about the performance of each method.

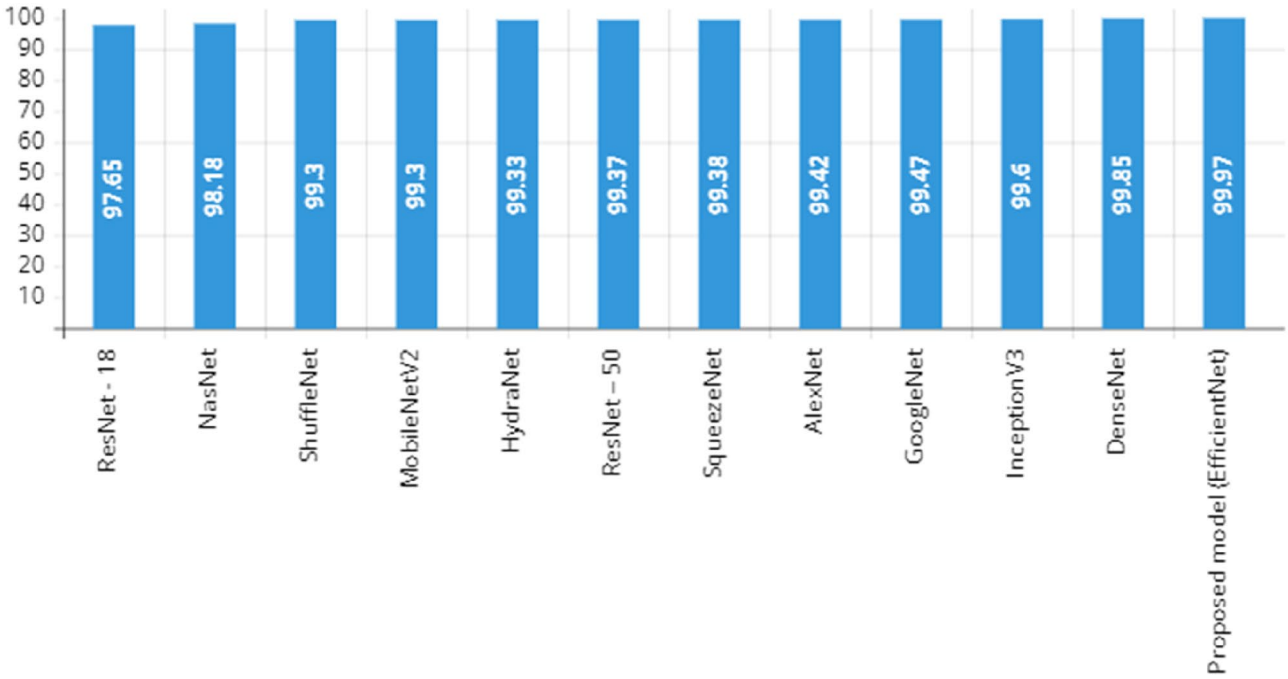

Fig. 13. Accuracy analysis.

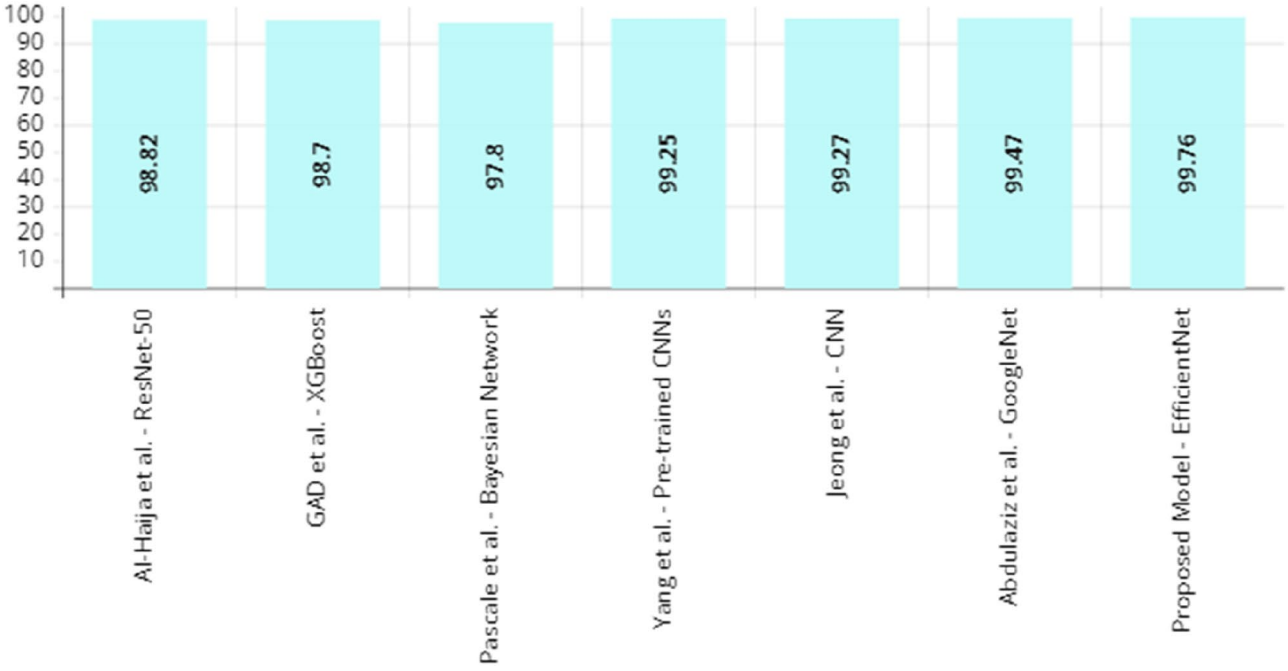

Fig. 14. Comparison with existing ML models.

Conclusion

Smart cities have integrated advanced technology and data analytics to maximize urban operations, promote sustainability, and improve people's lives. In this ecosystem, self-driving cars play a critical role because they are effective, secure, and environmentally friendly means of transportation. The development of 6G technology highlights their potential to transform autonomous vehicle systems. The integration of an intelligent dynamic threat detection system within 6G-enabled autonomous vehicle networks represents a critical advancement in securing communication in cyber-physical systems. The proposed system, which leverages advanced machine learning techniques and real-time data processing, offers a robust solution to detect and neutralize cyber threats that could compromise the safety and functionality of autonomous vehicles. After analysis and comparisons it

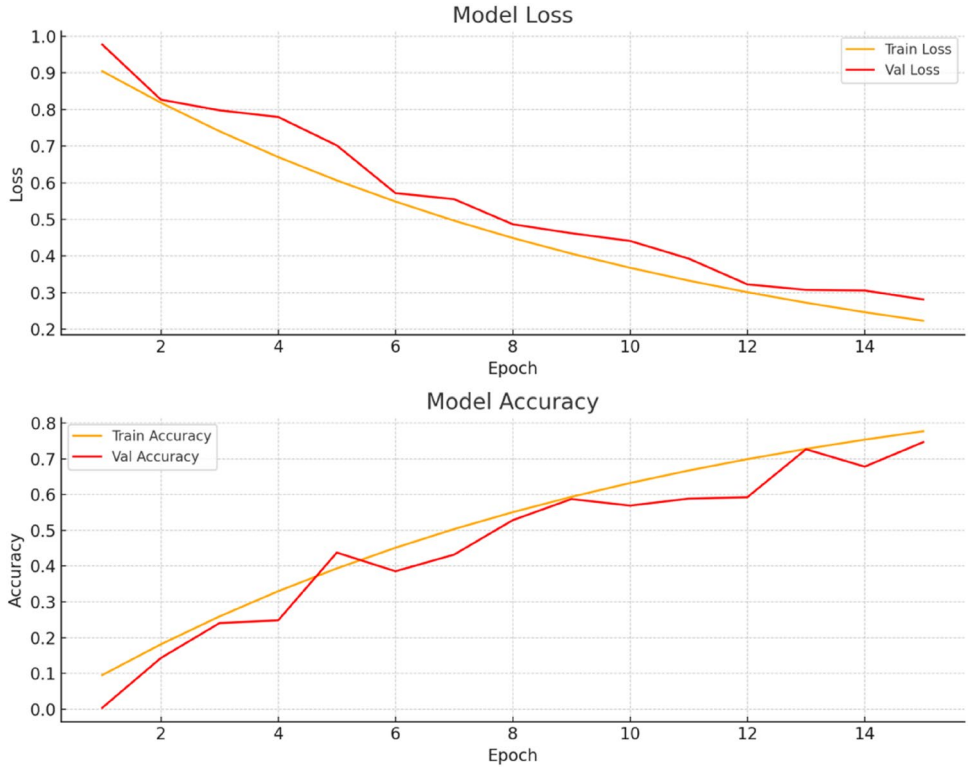

Fig.15. Training and validation loss & Training and validation accuracy of ResNet-18.

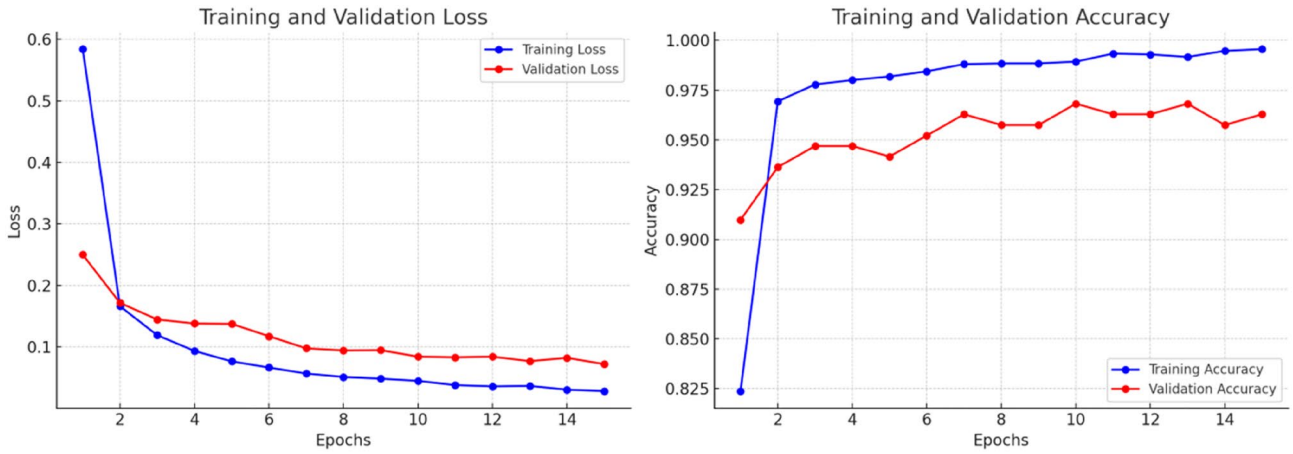

Fig.16. Training and validation loss & Training and validation accuracy of ResNet-50.

was found that EfficientNet stands out as the model providing improved performance and reliability necessary for the safety focused tasks of autonomous vehicles.

Thus this research proves that EfficientNet emerges as the best model with an incredible accuracy of up to 99.97%.By ensuring secure communication channels and proactively addressing potential vulnerabilities, this approach not only enhances the reliability of autonomous vehicles but also sets a new standard for security in next-generation vehicular networks.

Future work

The proposed work can be further improved by employing federated learning along with smart grids for efficient identification of intrusion in CPS and 6G cellular networks. Moreover, the scalability of the proposed work can be improved by using heterogeneous devices which provides seamless connectivity of all the devices that are connected in 6G network.

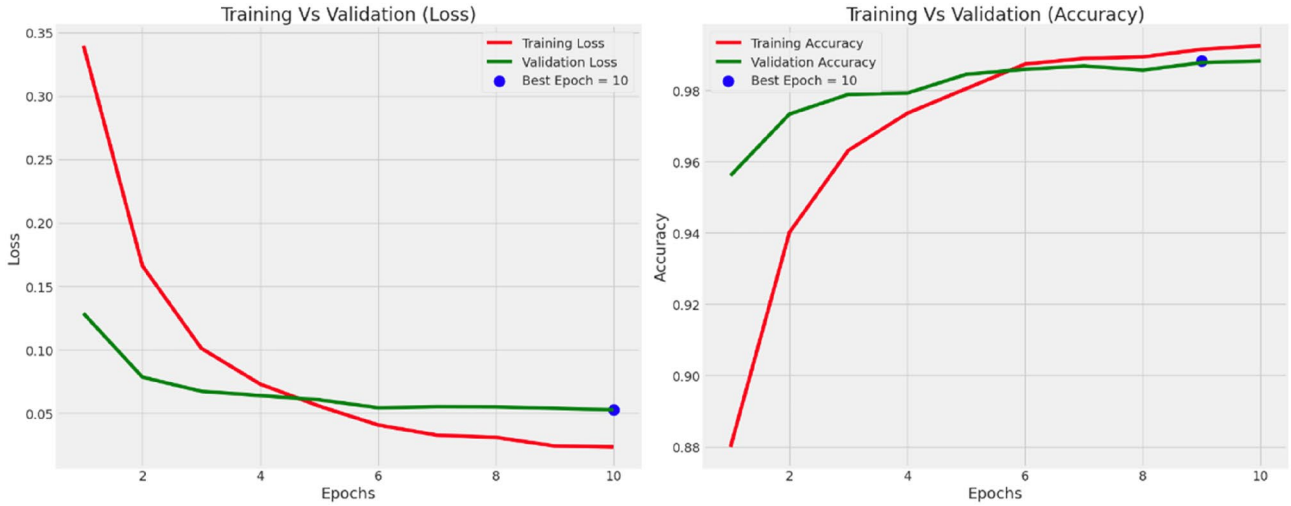

Fig.17. Training and validation loss & Training and validation accuracy of AlexNet.

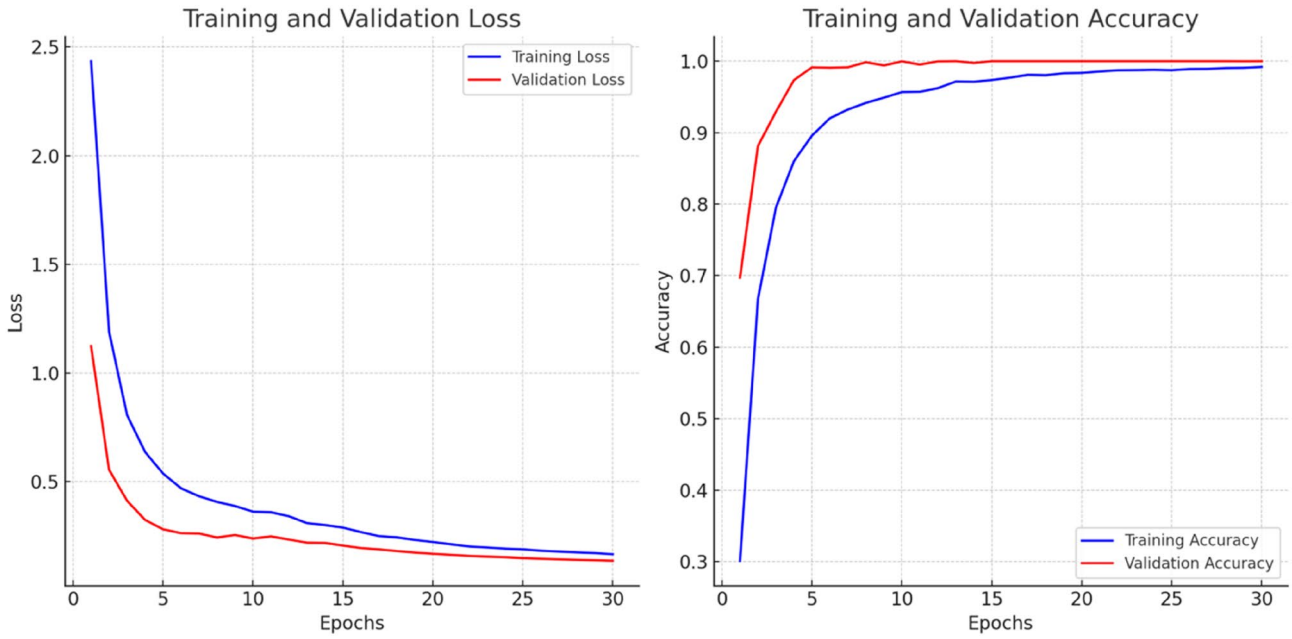

Fig.18. Training and validation loss & Training and validation accuracy of InceptionV3.

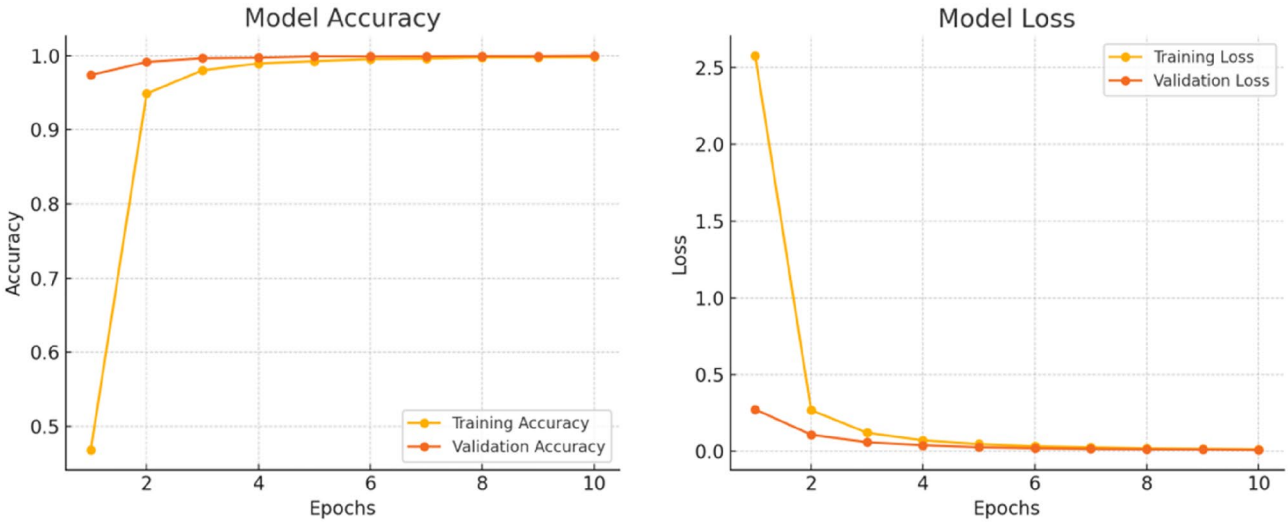

Fig.19. Training and validation loss & Training and validation accuracy of DenseNet.

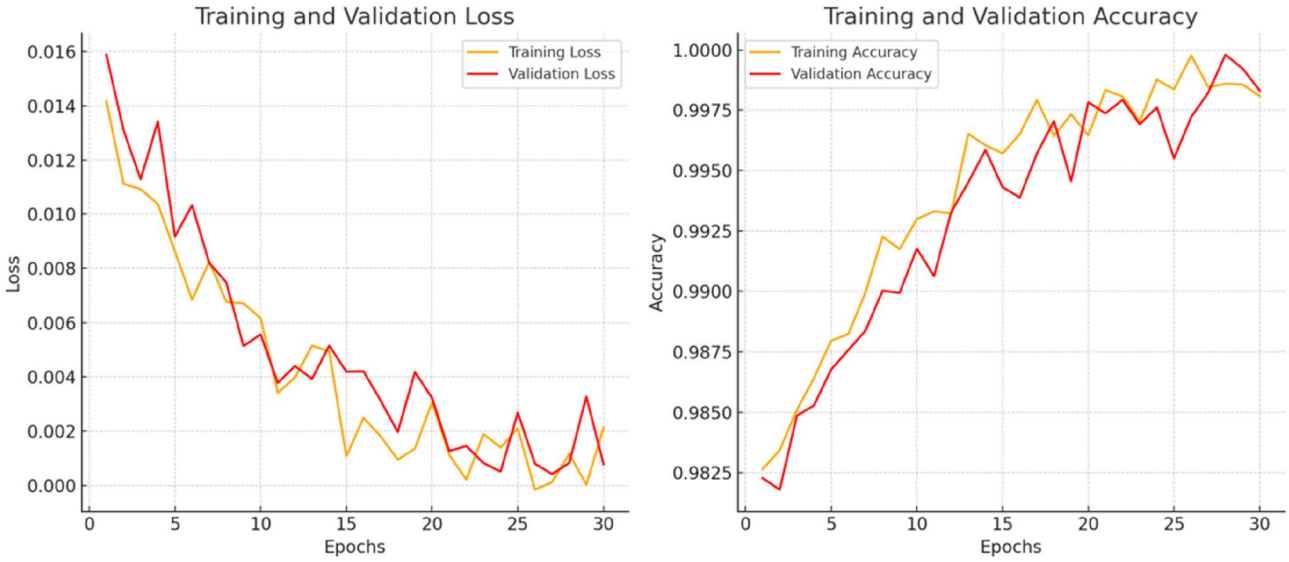

Fig.20. Training and validation loss & Training and validation accuracy of EfficientNet (Proposed Model).

Model name	Accuracy	Precision	Recall	F1—Score	Estimated computation cost (in GPU hours)
ResNet—18	97.65	96.42	98.59	97.29	5
NasNet	98.18	97.27	98.7	98.05	10
ShuffleNet	99.30	99.46	98.62	98.44	6
MobileNetV2	99.30	99.49	98.62	99.04	8
HydraNet	99.33	99.76	98.2	99.12	7
ResNet – 50	99.37	99.45	98.75	98.82	9
SqueezeNet	99.38	99.61	98.78	99.05	8
AlexNet	99.42	99.62	98.85	98.98	11
GoogleNet	99.47	99.69	98.94	99.04	8
InceptionV3	99.60	99.75	98.75	99.15	10
DenseNet	99.85	99.78	97.1	99.6	13
Proposed model (EfficientNet)	99.97	99.83	98.6	99.76	12

Table 1. Outcomes pertaining to the accuracy of performance.

Research paper	Methods	Performance	Metric
Al-Haija et al	ResNet-50	98.82	F1-Score
GAD et al	XGBoost	98.70	F1-Score
Pascale et al	Bayesian Network	97.80	F1-Score
Yang et al	Pre-trained CNNs	99.25	F1-Score
Jeong et al	CNN	99.27	F1-Score
Abdulaziz et al	GoogleNet	99.47	F1-Score
Proposed model	EfficientNet	99.76	F1-Score

Table 2. Comparison of few industry-leading ML models along with comparison criteria.

Data availability

The data that supports the findings of this research work are available from the corresponding author upon reasonable request.

Received: 9 June 2024; Accepted: 21 August 2024
Published online: 05 September 2024

References

1. Al-Haija QA, Smadi MA, Zein-Sabatto S (2020) Multi-class weather classification using resnet-18 CNN for autonomous IOT and CPS applications. *International Conference Computational Science and Computational Intelligence (CSCI)* 2020:1586–1591. https://doi.org/https://doi.org/10.1109/CSCI51800.2020.00293.
2. 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.
3. *International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2023, pp. 1252-1257, https://doi.org/10.1109/ICICCS56967.2023.10142687.
4. Bizon, N., Dascalescu, L., Tabatabaei, M. & Naser,,. *Autonomous Vehicles: Intelligent Transport Systems and Smart Technologies* (Nova Science Publishers Inc, Series, 2014).
5. Shi, Y., Lv, L., Yu, H., Yu, L. & Zhang, Z. A center-rule-based neighborhood search algorithm for roadside units deployment in emergency scenarios. *Mathematics* **8**, 1734. https://doi.org/10.3390/math8101734 (2020).
6. Natheeswari, N., Sivaranjani, P., Vijay, K. & Vijayakumar, R. Efficient data migration method in distributed systems environment. *Adv. Parallel Comput.* **37**, 533–537 (2020).
7. Ali Alheeti, K. M. & McDonald-Maier, K. Intelligent intrusion detection in external communication systems for autonomous vehicles. *Syst. Sci. Control Eng.* **6**(1), 48–56 (2018).
8. Mahmoud, O. *et al.* A feature selection method for classifcation within functional genomics experiments based on the proportional overlapping score. *BMC Bioinform.* **15**, 274. https://doi.org/10.1186/1471-2105-15-274 (2014).
9. 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.
10. Alsulami, A. A., Abu Al-Haija, Q., Alqahtani, A. & Alsini, R. Symmetrical simulation scheme for anomaly detection in autonomous vehicles based on LSTM model. *Symmetry* **14**, 1450. https://doi.org/10.3390/sym14071450 (2022).
11. Philipsen SG, Andersen B, Singh B (2021) Threats and Attacks to Modern Vehicles. In: *IEEE International Conference Internet Things and Intelligent Systems (IoTaIS)* 2021:22–27. https://doi.org/10.1109/IoTaIS53735.2021.9628576.
12. 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/10.5220/00077 26004750482.
13. 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.
14. Shanthalakshmi, M., Jananee, V., Perumal, P. N. & Jayakar, S. M. September). Identification of casting product surface quality using alexnet and lenet CNN Models. *J. Phys. Conf. Ser.* https://doi.org/10.1088/1742-6596/2335/1/012031 (2022).
15. Yang, L., Moubayed, A. & Shami, A. 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 (2022).
16. Omar Minawi, Jason Whelan, Abdulaziz Almehmadi, and Khalil ElKhatib. 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
17. 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, 10.1109/UEMCON53757.2021.9666745
18. 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
19. Liu, Y. *et al.* Interaction-enhanced and time-aware graph convolutional network for successive point-of-interest recommendation in traveling enterprises. *IEEE Trans. Ind. Inf.* **19**(1), 635–643. https://doi.org/10.1109/TII.2022.3200067 (2023).
20. Anbalagan, S., Raja, G., Gurumoorthy, S., Suresh, R. D. & Dev, K. IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* https://doi.org/10.1109/TITS.2023.3271768 (2023).
21. CPSRC - UCSC. (2018, May 23). *What are cyber physical systems? [Video]*. YouTube. https://www.youtube.com/watch?v=C6q88zJwq2g
22. Simplilearn. (2022b, May 27). *What is Intrusion Detection System? | Intrusion Detection System (IDS) | Cyber Security |Simplilearn* [Video]. YouTube. https://www.youtube.com/watch?v=dfVAi87BSEs

23. India Science. (2023, April 8). *Cyber Physical system* [Video]. YouTube. https://www.youtube.com/watch?v=VhtFv6TtWBo
24. Journal, I. (2021). *Intrusion Detection System: an approach to Autonomous vehicles*.www.academia.edu. https://www.academia.edu/64696486/Intrusion_Detection_System_An_Approach_to_Autonomous_Vehicles
25. Alheeti, K. M. A. & McDonald-Maier, K. Intelligent intrusion detection in external communication systems for autonomous vehicles. *Syst. Sci. Control Eng.* **6**(1), 48–56. https://doi.org/10.1080/21642583.2018.1440260 (2018).
26. Aloqaily, M., Otoum, S., Ridhawi, I. A. & Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Netw.* **90**, 101842. https://doi.org/10.1016/j.adhoc.2019.02.001 (2019).
27. Birkinshaw, C., Rouka, E. & Vassilakis, V. G. Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *J. Netw. Comput. Appl.* **136**, 71–85. https://doi.org/10.1016/j.jnca.2019.03.005 (2019).
28. Vijayakumar, R., Vijay, K., Sivaranjani, P. & Priya, V. Detection of network attacks based on multiprocessing and trace back methods. *Adv. Parallel Comput.* **38**, 608–613 (2021).
29. Mathew, Dennise, G. Kirubasri, K. Vijay, I. Eugene Berna, and K. R. Sowmia. "System for Detecting Intrusions using Raspberry PI." In: 2023 *International Conference on Computer Communication and Informatics* (ICCCI), pp. 1–6. IEEE, 2023.
30. Shanthalakshmi, M., Gogoi, D., Chhabra, M., Rana, S. & Thakur, S. "A distributed malicious attack detection and prevention approach using honeypots in ad-hoc network "was published in SSRG International Journal of Computer Science and Engineering – (2'ICEIS-2017) –Special Issue–2017.
31. Sadaf, M. *et al.* A novel framework for detection and prevention of denial of service attacks on autonomous vehicles using fuzzy logic. *Veh. Commun.* **46**, 100741. https://doi.org/10.1016/j.vehcom.2024.100741 (2024).
32. Dr, A., George, S., Dr, T. & Baskar, & Dr.P. Balaji Srikaanth.,. Securing the self-driving future: Cybersecurity challenges and solutions for autonomous vehicles. *Partn. Univers. Innov. Res. Publ. (PUIRP)* **01**(02), 137–156. https://doi.org/10.5281/zenodo.10246882 (2023).
33. Dr, A. S., George, A. S., George, H. & Baskar, T. Wi-Fi 7: The next frontier in wireless connectivity. Partn. Univers. Int. Innov. J. https://doi.org/10.5281/zenodo.8266217 (2023).
34. Vinayagam, J., Murugan, S., Mishra, S., Samuel, L. J., Prabakar, R., & Shalini, M. (2023, August). An approach for devising stenography application using cross modal attention. In *AIP Conference Proceedings* (Vol. 2790, No. 1). AIP Publishing.
35. 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.
36. S. K. D et al., "Implementation of Smart Vehicle Accident Detection using Raspberry PI in Smart Cities," *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2022, pp. 1611-1614, https://doi.org/10.1109/ICIRCA54612.2022.998576
37. Vinayagam, J., Murugan, S., Jesu, S. G., Vaidhya, G. K., Narayanan, N. S., & Thayil, N. B. (2023, August). Detection of diabetic retinopathy using AlexNet and lenet CNN models. In AIP Conference Proceedings (Vol. 2790, No. 1). AIP Publishing.
38. 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.
39. Zhang, L. & Ma, D. 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 (2022).
40. Intrusion detection system using machine learning for vehicular ad hoc networks based on TON-IoT dataset. (2021). *IEEE Journals & Magazine* | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9576115/
41. Zhu, Z., Hu, Z., Dai, W., Chen, H. & Lv, Z. Deep learning for autonomous vehicle and pedestrian interaction safety. *Saf. Sci.* **145**, 105479. https://doi.org/10.1016/j.ssci.2021.105479 (2022).
42. Song, H. M., Woo, J. & Kim, H. K. In-vehicle network intrusion detection using deep convolutional neural network. *Veh. Commun.* **21**, 100198. https://doi.org/10.1016/j.vehcom.2019.100198 (2020).
43. Koonce, B. Convolutional neural networks with swift for tensorflow. In *Apress eBooks* (ed. Koonce, B.) (Springer, 2021). https://doi.org/10.1007/978-1-4842-6168-2.
44. AlEisa, H. N. *et al.* Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning. *IEEE Trans. Consum. Electron. 70*(1), 1736–1746. https://doi.org/10.1109/TCE.2023.3325827 (2024).
45. Mazhar, T. *et al.* Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. *Future Internet* **15**(2), 83 (2023).
46. Ghadi, Y. Y. *et al.* Integration of federated learning with IoT for smart cities applications, challenges, and solutions. *PeerJ Comput. Sci.* **9**, e1657 (2023).
47. Shah, S. F. A. *et al.* Applications, challenges, and solutions of unmanned aerial vehicles in smart city using blockchain. *PeerJ Comput. Sci.* **10**, e1776 (2024).
48. Ghadi, Y. Y. *et al.* Machine learning solution for the security of wireless sensor network. *IEEE Access* https://doi.org/10.1109/ACCESS.2024.3355312 (2024).
49. Khan, I. A. *et al.* A new explainable deep learning framework for cyber threat discovery in industrial IoT networks. *IEEE Internet Things J.* **9**(13), 11604–11613 (2021).
50. Khan, I. A. *et al.* An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles. *IEEE Trans. Intell. Transp. Syst.* **23**(12), 25469–25478 (2021).
51. Khan, I. A. *et al.* A privacy-conserving framework based intrusion detection method for detecting and recognizing malicious behaviours in cyber-physical power networks. *Appl. Intell.* https://doi.org/10.1007/s10489-021-02222-8 (2021).
52. Liu, Z. *et al.* Establishing trustworthy and privacy-preserving SAGIVNs in 6G: architectures, requirements, and solutions. *IEEE Netw.* **38**(2), 141–147. https://doi.org/10.1109/MNET.2023.3335974 (2023).
53. J. Manikandan, S. R. Devakadacham, M. Shanthalakshmi, Y. Arockia Raj and K. Vijay, (2023)"An Efficient Technique for the Better Recognition of Oral Cancer using Support Vector Machine," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 1252-1257.
54. Anandhi, S., Devakadacham, S.R., Manikandan, J., Shanthalakshmi, M.(2024), Enhancing Lung Disease Diagnosis through Meta Learning: A Framework Utilizing Few-Shot Learning Techniques, Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024.
55. Keerthana, S., Deepika, N., Pooja, E., Shanthalakshmi, M., Khanaghavalle, G.R.(2024), An effective approach for detecting deepfake videos using Long Short-Term Memory and ResNet, 2024 International Conference on Communication, Computing and Internet of Things, IC3IoT 2024 - Proceedings, 2024.
56. Liu, Z. *et al.* PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks. *IEEE Trans. Veh. Technol.* https://doi.org/10.1109/TVT.2023.3340723 (2023).
57. Guo, J. *et al.* TROVE: A context-awareness trust model for VANETs using reinforcement learning. *IEEE Internet Things J.* **7**(7), 6647–6662 (2020).

Author contributions

M.S confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation. R.S.P reviewed the results and approved the final version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.M. or P.R.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.