Research Article

Cyber-Physical Systems Security: A Comparative Taxonomy of Cyber Attacks And Defense Mechanisms In Smart Healthcare and Autonomous Vehicles

Dhivya Rathinasamy (Corresponding Author)[1] , R Swathiramya[2] , Vishnu Kumar K[3] , Sivaramakrishnan Rajendar[4] , Pandi M[5]

[1]Assistant Professor Department of Information Technology Dr.N.G.P Institute of Technology Coimbatore dhivya.rathinasamy@gmail.com
[2]Assistant Professor Department of Artificial Intelligence and Data Science Hindusthan Institute of Technology Coimbatore swathiramyaravichandran@gmail.com
[3]Professor Computer Science and Engineering KPR Institute of Engineering and Technology Coimbatore vishnudms@gmail.com
[4]Associate Professor Department of Computer Science and Engineering Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai drsivaramakrishnanr@veltech.edu.in
[5]Professor Department of Computer Science and Engineering Ramco Institute of Technology Virudhunagar mpandi123@gmail.com

Abstract:

Background: The rapid adoption of Artificial Intelligence (AI)-enabled Cyber-Physical Systems (CPS) has transformed modern healthcare by enabling intelligent patient monitoring, remote diagnosis, wearable health devices, robotic assistance, and real-time clinical decision-making, alongside analogous cyber-physical structures in autonomous ground vehicles (AGVs) real-time clinical decision-making. While these technologies improve healthcare quality and accessibility, their increasing connectivity exposes healthcare infrastructures to a wide range of cyber threats that may compromise patient safety, privacy, and clinical operations.

Methods: This review presents a comprehensive taxonomy of cyber-attacks targeting AI-driven healthcare CPS, including attacks on sensors, communication networks, cloud platforms, medical Internet of Things (IoMT) devices, AI algorithms, and control systems, as well as AGV components such as ECUs, CAN networks, and onboard sensors (LiDAR, RADAR, camera, GPS) AI algorithms, and control systems. Recent research on intrusion detection, encryption techniques, blockchain, federated learning, explainable AI, trust management, and zero-trust architectures is systematically analyzed to evaluate existing defense mechanisms.

Results: The review identifies major vulnerabilities across healthcare and AGV CPS components and summarizes current mitigation strategies designed to improve system resilience, data integrity, patient privacy, and operational reliability. Furthermore, emerging AI-based security solutions capable of detecting sophisticated attacks in real time are critically discussed.

Conclusion: Although significant progress has been achieved in securing healthcare and AGV CPS, challenges remain in ensuring scalability, interoperability, regulatory compliance, and trustworthy AI deployment. Future research should focus on developing adaptive, intelligent, and privacy-preserving cybersecurity frameworks capable of supporting next-generation digital healthcare ecosystems.

Keywords: Artificial Intelligence; Cyber-Physical Systems; Smart Healthcare; Autonomous Ground Vehicles; Medical Internet of Things; Cybersecurity; Intrusion Detection; Healthcare Security; Data Privacy.

1 Introduction

In recent times the It's provides effective performance using intelligent decision making with real-time data. Autonomous Ground Vehicle (AGV) plays a vital role in the Intelligent Transportation System. Hence the production of AGVs is increased in large automobile manufacturing companies [1]. The enlargedgrowth in AGV manufacturing has resulted from amplified technical features and far-reaching consequences [2]. Due to the vehicles being autonomous and heterogeneous, these evolving technologies open up exciting gaps for research and development in the area of (i) handling security and privacy issues, improving performance and efficiency in complicated computational units, (iii) complex social communication between the vehicles and infrastructure, (iv) increase user's comfort [3]. Among all these challenges, delivering safety with better performance for AGV is the top concern [4]. In this review, the various security attacks in AGV that use the CPS approach are investigated with security mechanisms andrecommendation systems. Unlike traditional vehicles, AGV involves integrating sensing, control,

analysis,wireless communication, and computation technology of a massive volume of real-time data using a Cyber-Physical System (CPS) [5]. The levels of automation in an autonomous vehicle vary from human-operated to completely self-driving. Society of Automotive Engineers (SAE) is U.S. based, globally active professional association that provided a standard classification system that defined six different levels of automation, ranging from level 0 (no automation) to level 5 (full automation) [6]. Figure 1 shows the different levels of automation.

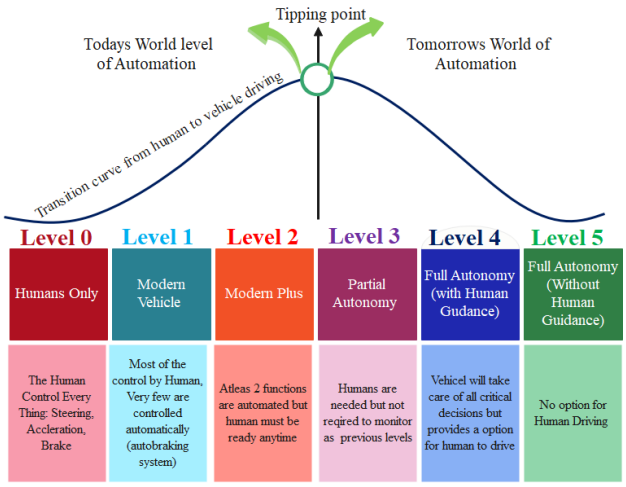


Figure 1: Levels of automation

The AGV developers were quietly extending the production rate for level 3, 4, and 5 vehicles. The pandemicsituation has also accelerated AGV usage. Nowadays, the Adoption of level 3 automation vehicles by users is increased dramatically. The BNEF'S Outlook for Advanced Driver Assistance System (ADAS) Adoptionreport [7] is shown in Figure 2 (a). Hence, the global market for Level 3 automation vehicles has increasedfrom $27B in 2020 to $83B in 2030, detailed in the Marketsonmarkets report. The AGV is developed by many major automobile manufacturers globally, such as BMW, Audi, Ford, Google, GM, Tesla, Volkswagen, and Volvo, focusing on emerging their software and hardware componenttechnologies. The overall automotive software market is poised to raise from $18B in 2018 to $52B by 2025 [8]. At present, Google spins off - Waymo is the only platform taking passengers in fully driverless vehicles. Figure 2 (b) shows the details of patents filed by the top automobile companies [9].

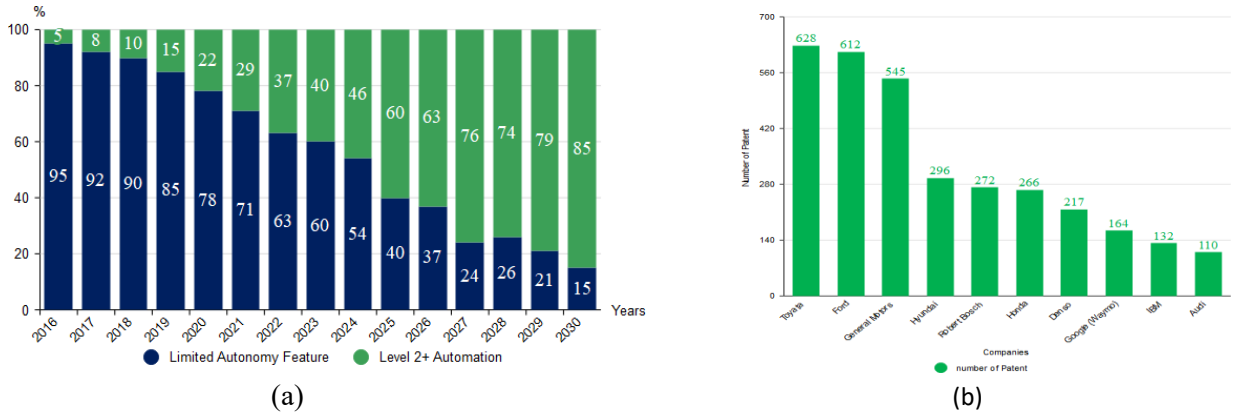


Figure 2: (a) BNEF'S Outlook for Advanced Driver Assistance System Adoption, (b) Top companieswith autonomous vehicles patents

The AGV depends on the onboard sensors data to decide while navigating to complete the desired task. Based on thelevels of automation variety of sensors are situated in different parts of the vehicle. Driver assistance systemis supported from level 3 AGV with at that minimum, three sensors, such as Lidar, Radar and Camera [10].Once the

vehicle learns accurate information about the environment and its position, the vehicle will have to commend speed and bearing. Automation is the result of a series of processes that loop from environmentdata acquisition, the process of data, control the vehicle. It makes sure the vehicle movement in the desiredpath [11]. Intelligent control algorithms are embedded in the controller to compute and take the decision locally, and the data are shared with the infrastructure for driving decisions. While doing this, there is the chance of risk and threats from attackers to compromise the entire operations remotely. To avoid such kinds of intrusions,the AGV should have some protection mechanism to enhance safety, efficiency, and reliability even though such mechanisms are compromised by the attackers and pose a high risk, leading to catastrophic damage tothe environment and vehicle.

AGV can be compromised by the attackers where they control and manipulate the data being shared internally and on the infrastructure. In the countries like USA, U.K., and South Korea, people got positivethoughts about using AGV as public transport since the pandemic. However, the main concern is that thesevehicles are safe. These concerns created a significant eye-opener for the researcher's community to understand the attackers' threats and find solutions. The usage of AI in AGV has become popular nowadays specifically as a security mechanism and identify and avoid possible security threats while the AGVs are on roads [12][13]. In AGV, the technology uses sensor data for all actions. Using these data, a RecurrentNeural Network (RNN) based on an AI anomaly detection system learns to recognize patterns of differentsituations. If the system identifies a new pattern than the expected one, then it is investigated. The anomalydetection techniques are based on a threshold, Statistical, nearest neighbor, cluster, classification, and perdition algorithms [14][15]. The novelty of this paper lies in its focus on the security challenges specific to connected AGVs, offering a detailed examination of vulnerabilities and defenses that may not be covered in broader surveys. The motivation behind this survey is to address the urgent need for improved security in AGVs due to their increasing use and the potential risks associated with remote attacks. This survey is valuable to researchers, developers, and policymakers as it provides insights into the latest developments in AGV security, helping them understand the current state of the field and guiding their efforts in enhancing AGV security. The following is the contribution to this paper.

- The possible attacks related to AGV towards the CPS approach are reviewed and discussed in detail.The state-of-the-art attacks and protecting mechanisms in CPS-based AGV are studied.
- Future research directions pretending to develop a control system for AGV with a defense mechanism are proposed.

2 Artificial Intelligence-based AGV – CPS approach

Artificial intelligence is the fundamental functional unit for streamlining traffic management & decision- making systems in ITS. The applications of AI in ITS are not limited, including decision support systems,law enforcement capacities, traffic demand monitoring, traffic signal control, and the fixable AI-based traffic flow prediction approaches [16][17]. Cyber-Physical System (CPS) is a multidisciplinary system that integrates physical entities with cyber capability through computation, communication and control technologies to improve performance. Artificial Intelligence methods are used in controlling the physical components of the vehicle. With the aid of CPS, the Intelligent Transportation System aims at constructingintelligence across these domains by bridging the physical components and processes with the cyber worldto improve road transportation efficiently in terms of time, speed, security, safety[18]. The Cyber-Physical Systems units monitor and control physical processes utilizing sensors, actuators, and control systems. Thefunctionality of one component is very much dependent on other components [19]. Fig 3 illustrates the general workflow of the Cyber-Physical System. There are three layers in CPS responsible for four primaryoperations, namely monitoring, networking, controlling, and actuation. Layer 1 has a controller unit, layer2 has an actuator and sensor, and layer 3 has a physical plant. Firstly, the mechanical plant's physical process and environment are monitored, and the feedback on actions done by the mechanical plant is taken for corrective actions in the future. Different sensors are used in CPS to collect real-time data, which are aggregated or diffused for analysis. This process is known as networking. The collected data are analyzed with various algorithms in the controlling phase to determine whether the physical practice satisfies the pre-defined criteria. If it is not contented, the corrective actions are proposedto be accomplished to meet the criteria. Finally, the proposed action is executed by the actuator.

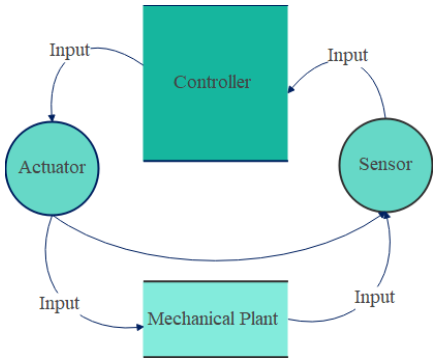


Figure 3: The general workflow of Cyber Physical System approach for AGV

The controller processes massive data. The static and dynamic data is processed by using artificial intelligence techniques to produce accurate decision. Different security vulnerabilities are possible in all three layers ofCPS [20].

2.1. Layer 1: Controller of CPS in AGV

The control algorithms used in the CPS is to provide the right decision while the AGV is moving in the unknown environment. One of the significant advances using the AI-based control system is to have the ability to access the environment with the active sensor and to make the right decision better than the human driver. The advanced features of AGV are organized primarily by computation and communication units inthe AGV, such as Electronic Controller Unit (ECU) and Controller Area Network (CAN). ECU is a microcontroller that is commended by embedded software. Typically, one ECU can support a minimum of any one of the applications of AGV such as steering control, engine control, airbag, window lifter [21]. Hence, the most advanced driver vehicles with nearly thirty to a hundred discrete electronic control units (ECU) will become increasingly sophisticated and morph into a full-blown autonomous driving system [22]. The ECU utilize complex algorithms like machine learning, deep learning to generate accurate results [23]. Three types of machine learning algorithms are used to accomplish the tasks in ECU.They are supervised algorithms like regression, classification and anomaly detection, unsupervised algorithms like association, rule learning and clustering, and reinforcement algorithms. The Controller Area Network (CAN) communicated like the peer-to-peer network used for the serial communication between the devices in the autonomous vehicles [24]. The typical CAN frames contain SOF,Arbitration, control, payload, CRC, ack, and end of a frame. Table 1 exemplifies the controllers and usage of AI in AGVs.

Table 1: Controllers and AI model adopted in AGV

Controller	AI Model	Feature	Drawbacks
Door control unit [25]	Regression methods	Controlling and monitoring window movements	Power failure
Engine control unit [26]	Regression and classification methods	optimal engine performance	Expensive
Speed control unit[27]	hybrid fuzzy sliding mode control	Auto cruise the vehicle	Generation of Harmonic currents.
Telematic control unit [28]	Predictive maintenance algorithm	Connects the vehicle to cloud services	Privacy concerns

2.2. Layer 2: sensory data of AGV

The two main leads of autonomous cars are sensors and actuators, which are necessary to thwart the human interaction for driving.*Actuator in AGV* - Lots of sensors gather the surrounding dynamic conditions information. Based on the sensor and controller input, the processors in AGV will direct the actuator to perform physical actions likeacceleration, direction, and stop [29]. *Sensor Technology in AGV* - The sensors play a vital role in perceiving the surroundings of the vehicle. Thesensors are classified as passive and active sensors [30] [31]. A passive sensor senses

the surrounding energyand produces the outputs. Cameras and GPS are examples of Passive sensors. On the other hand, Active sensors diffuse the energy and measure the reflected energy to produce the outputs. Lidar and Radar are examples of Active sensors [32]. Table 2 describes the various sensors used in Autonomous Ground Vehicles (AGV).

Table 2: Comparison of sensor used in AGV

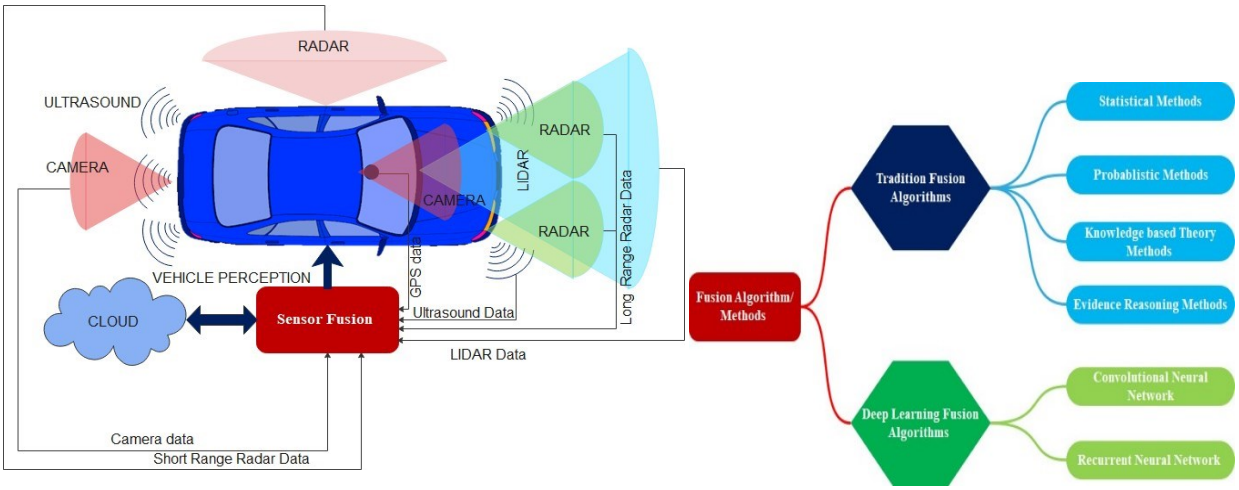
Sensor Type	Waves	Frequency	Range	Feature	Drawback	Manufactures	Type of sensor
Ultrasonic Sensors [33]	ultrasonic	20-40 kHz	11m	Detected transparent and non-metal objects	Avail for short-range, Measurement with noise	Siemens, Process Instrumentation, IFMEfector, Inc. B&B Instruments Inc.	Active
RADAR [34]	Radio	67 – 81 GHz	5m-200m	velocity and direction of objects	Not good for metalobjects, Low-resolution images	Fujitsu, BYDA Acconeer AB, Farran	Active
LIDAR [35]	Light	935-1550 THz	200m	Vehicle localization	Influenced by weather conditions, expensive	Hexagon AB, Velodyne Lidar Sick AG, Topcon Positioning Systems,Inc.	Active
Monocular camera [36]	Light	30fps	250m	dimension ofobject	Need high output processing power, Influenced by weather	PULSAR, FLIR Systems, NightOwl	Passive
Stereo camera [37]	Light	30fps	250m	Object depth measurement			
					High price, Low rangedetection, Hard to implement	Autoliv Inc, Continental AG. Hisense, International Co. Ltd,Hitachi Ltd	Passive

Sensor fusion Technology- Sensors need more precise data from sensors to better understand the surroundings [38] [39]. To overcome the limitations and increase efficiency in the individual sensors, sensor fusion combines data from the different sensors. The need for sensor fusion is detailed in table 3.

Table 3: Sensor Comparison based on Characteristics (* Good, ~ Average, ∞Bad)

Sensor	Range	Resolution	Distance Accuracy	Colour Perception	Object detection	Object Classification	Edge detection	Lane Detection	Weather Condition
Ultrasonic	~	~	*	∞	*	*	∞	∞	∞
RADAR	*	∞	*	∞	*	∞	∞	∞	*
LiDAR	~	~	*	∞	*	~	*	∞	~
Camera	~	*	~	*	~	*	*	*	∞
* Good, ~ Average, ∞Bad									

Some obstacles in sensor fusion are multimodal data, heterogeneity, data uncertainty, and data spoofing attacks [40]. In [6], the combined LiDAR data and camera and applied a classifier algorithm for getting better resolution images. In existing navigation prediction methods, traditional and deep learning fusion algorithms are used. Figure 4(a) and (b) shows the sensor fusion and classification of fusion algorithms.



(a) (b)

Figure 4: (a) The conceptual sensor fusion in AGV, (b) Classification of Fusion Algorithms

2.3 Layer 3: Physical Plant of AGV

All the hardware components of the vehicles are known as physical plant unit. Based on the controllerinput, the actuator will kindle the physical components. The results of all sensor, actuator and controller functionalities are shown in the physical plant.

3 Vulnerable Components Attacks in AGV

The overall classification of different component attacks in AGV is exemplified in figure 5.

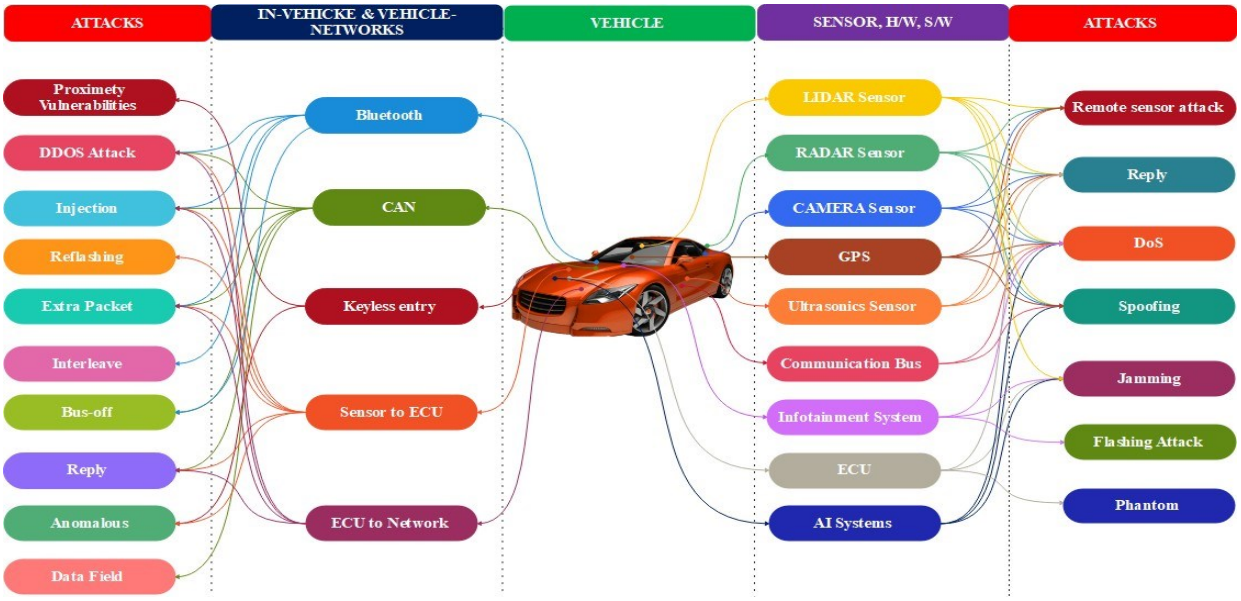


Figure 5: Classification of component attacks in AGV

3.1. Controller attacks

Electronic Control Units are the most critical units in the control system, which controls the signal transmission and manages the sensors in AGV. All parts of the AGV is connected via the in-vehicle networkcalled as CAN [41].

ECU software flashing attacks - The numerous ECUs are available like engine ECU, transmission ECU, Airbag ECU, steering ECU, Etc. providing data security for ECU is more critical. For instance, remotely disable Electronic Control Unit (ECU) or ADAS by faking or flooding the sensor information. Such kindsof attacks are considered most dangerous since the attacker can control the autonomous vehicle activity [42] [43]. ECU attacks are broadly classified as front door attacks (Compromising the access mechanism), backdoor attacks (hardware hacking), and exploits (unintentional access), respectively [44]. In [45] Smith. C explained the ECU Attacks re-flashing and ECU-remapping.

CAN attacks - The CAN bus is used to pass the commands inside the vehicle to control. In Controller AreaNetwork, two types of attacks can be possible: Denial of Service Attack and Modification of message attacks such as injection, reflash, extra packet, Interleave, drop, discontinuity, and unique Reverse [46][47][48]. In Trend Micro technical brief [49], three different threat scenarios based on DoS attacks such as Active Safety System DoS, Throttle DoS, Door Lock DoS were explained and recommendations such as Network Segmentation or Topology Alteration, Regulated OBD-II Diagnostic Port Access and Encryptionwas suggested. In [50], the various possible security attacks in Controller Area Network was described andmentioned that CAN attacks are possible due to the lack of authentication, network segmentation, and encryption. Table 4 summarizes the CAN attacks in AGV.

Table 4: Summary of CAN attacks in AGV

Ref	Type of attack	Security Mechanism	DoS attack	Modification Attack
[51]	Five kinds of anomalies (Interleave, drop,discontinuity, unusual, Reverse)	LSTM Neural Network Anomaly Detection model	-	✓
[52]	Extra packet insertion	Flow-based Anomaly Detection	✓	
[48]	bus-off attack	Weeping CAN	-	✓
[53]	Injection and reflash attacks,	time-defined window approach with unsupervised methods	-	✓
[54]	Data field attacks	Distributed anomaly detection system using hierarchicaltemporal memory (HTM)	-	✓
[55]	Anomalous bus messages.	Anomaly Detection Using a Deep Neural Network	-	✓
[56]	DoS, Replay attack	Hybrid Security System	✓	-

3.2. Sensor and actuator attacks

The complicated employment of high-tech sensors and algorithms are in autonomous vehicles directs to make autonomous decisions. At the same time, the possibility of attacks is also high [57]. Attackers remotely target millions of vehicles simultaneously, which causes crashes and leading to loss of vehicle infrastructure [58]. Most of these active and passive sensors are used for navigation purposes in AGV. Mostof the sensor attacks will have an abrupt impact on the navigation system. Making the target component inaccessible by flooding the data with traffic is a DoS attack. Intercepting the media age and then unfairly delays or resends it to misdirect the receiver is a replay attack. A jamming attack accumulates noise in theenvironment using some hardware device, and a spoofing attack injects the fabricated signals using a hardware device [59]. In [60], Jamal Raiyn described the summary of various cyber-attack scenarios relating to autonomous vehicles. As per his concern, the attackable components for an autonomous vehicle include a sensor network, camera, Global Positioning System (GPS), LiDAR, wireless communication. Kui Ren [4] classified the various types of cyber-attacks in an autonomous vehicle in three main categories suchas (1) In-vehicle system attacks – VCS, Immobilizer, keyless entry, Critical components (2) In-vehicle protocol – CAN, LIN, FlexRay (3) Various system – Camera, LiDAR, Radar, Ultrasonic sensor, GPS. ForBetter location identification, satellite-based

augmentation systems (SBASs), assisted-GPS, anddifferential-GPS are used. This unencrypted data and code are attackable [61]. Table 5 provides the summary of sensor attacks in AGV.

Table 5: Summary of sensor and actuator attacks in AGV

Attack	Compromised sensor	Description – mechanism	Consequence
Jamming attack	LIDAR [62]	Use strong lights to reflect the origin light tobottlenecks the LiDAR	Detection performance will decrease
	RADAR [62]	Use noise to damage the signals of RADAR	Surrounding environment deduction fails
	Camera [62]	Blind vision and fake image injection insensory data	The performance of the navigation system will degrade
	Ultrasonic Sensors [62]	Use noise to damage the signals ofUltrasonic Sensors	Poor detection rate in parking assistance system
	GPS [62]	Sends the powerful signal to ignore originalGPS signal	It will affects the Navigation coordination system
Replay attack	LIDAR [63]	Replaying the laser pulses with differentposition points	Localization will get affected
	RADAR [64]	Creating fake echo and signals	Make real objects are too close or far
	Camera [64]	Blinding the camera either fully or partially	Damaging the auto exposure control
	GPS [65]	Sends relative signals to the target	Making the traffic collision
Spoofing attack	LIDAR [6 3]	Manipulate the targeted sensor readings	Localization will get affected
	RADAR [66]	Replication and retransmission of signals	Velocity falsifying – increase collision
	Camera [67]	Alter the range measurements	The performance of the navigation system will degrade
	GPS [6 2]	Send signals to hoodwink the target vehicle	Guide the false location or route
DoS attack	LIDAR [68]	Making delay in signals	Misleading in object perception
	RADAR [69]	Retransmit the signal with added power	Affects the distance and velocity measurement.
	Camera [70]	Suspending or preventing commends for thetarget component	Making conflict in commends
	GPS [71]	Delaying the signals to reach the target	Mapping the location gets affected
	GPS [57]	Increase number of users at certain location	Route traffic in certain direction

3.3. Physical plant attacks

Physical attacks that tamper directly with physical elements in the CPS [72]. The physical attacks areclassified as invasive and non-invasive [69]. Physically damage the hardware components of the vehicle isknown as an invasive attack. For instance, they are disconnecting the battery cable of the airbag system inan automated vehicle. It can be

avoided by parking the car safely, driving the car by trusted persons, usinganti-theft devices, and turning the engine off when not in use [73]. Rather than direct physical damage, shoot up malicious data and signals into the vehicle's hardware is known as a non-invasive physical attack.Jamming attacks and spoofing attacks are examples of the non-invasive type. This attack is further classifiedas passive (observing) and active (modifying) attacks.

3.4. Attack – motivation

As for as, different attackable scenarios were explained. All those mentioned attacks will affect system security parameters such as integrity, confidentiality and privacy, availability, authentication, and authorization [74] [75]. Table 6 summarizes the possible cyber-attacks in autonomous vehicles.

Table 6: Possible cyber-attacks in autonomous vehicles in terms of security parameters: A-Integrity B-Confidentiality C-Privacy D-Availability E- Authentication F- Authorization

Reference	Year	Vehicle – part	Attack	Consequence	Attacker motive to compromise the security parameters					
					A	B	C	D	E	F
			split-second phantom attacks		✓	×	×	✓	×	×
Karl Koscher, et al. [22]	2010	ADAS	Replay attack	Driving functions	✓	✓	×	✓	×	✓
			Masquerade, injection attacks	fail,Collision	✓	✓	×	×	×	✓
			Traffic analysis		×	✓	✓	×	×	×
			Spoofing attack Jamming	Driving functions fail,						
Jamal Raiyn, et al. [60]	2018	LIDAR	Hidden objects,	Data theft, Vehicletheft, Collision	✓	✓	✓	✓	×	✓
			Fake objects							
Xingxing Guang, et al. [76]	2018	IMU	Deception attacks	Data theft, Vehicletheft, Collision	✓	✓	✓	✓	×	✓
Simon Parkinson, et al. [43]	2017	GPS	Spoofing attack	Data theft, Vehicletheft, Collision	✓	✓	✓	✓	×	✓
			Off the shelf attacks							
Shawn Carpenter, et al. [34]	2018	RADAR	Spoofing attack, Jamming	Data theft, Vehicle theft, Collision	✓	✓	✓	✓	×	✓
			Hidden objects, Fake objects							
Jin Cui et al. [34]	2015	ECU	sniffing, fuzzing	Data theft						
			replay and DoS attacks.	Vehicle systems	✓	✓	×	×	×	✓
			masquerade injection attacks	fail Driving functions fail						
			interception	Data theft	×	✓	✓	×	×	×
			Modification, fabrication	Vehicle systems	✓	×	×	✓	✓	×
Chung-Wei Lin, et al. [47]	2012	CAN	CAN sniffing, CAN fuzzing	fail Driving						
			DoS attacks DoS / DDoS	functions fail	✓	✓	×	✓	×	✓

Keshav Bimbraw, et al. [72]	2015	USB	CAN replay injection attacks Include malicious boot virus	Commercial loss Vehicle systems fail	✓	✓	×	×	×	✓
M Furqan Ayub, et al [61]	2018	Camera	Spoofing attack, Jamming, Hidden objects, Fake objects	Driving functions fail, Collision	✓	✓	✓	✓	×	✓
Francillon B. Danev, et, al. [77]	2011	Audio / Video Systems	Repackaging attacks, Update attacks, Eavesdropping, Sniffing.	Commercial loss, Vehicle systems fail, Driving functions fail	✓	✓	×	✓	×	✓
Amara Dinesh Kumar, etal. [78]	2018	Battery	Denial of Service attack	Commercial loss, Vehicle systems fail	×	✓	×	✓	×	×
Siegwart R, et al. [79]	2011	Mobile Device	Repackaging attacks, Update attacks, Eavesdropping, Sniffing.	Driving functions fail Commercial loss Data theft	✓	✓	×	✓	×	✓
Jairo Giraldo, et al. [80]	2018	Charging Interface	Eavesdropping, Sniffing.	Vehicle systems fail Commercial loss	×	✓	×	✓	×	✓
Abdullahi Chowdhury, etal. [68]	2020	OBD – II	Repackaging attacks, Update attacks, Eavesdropping, Sniffing.	Vehicle systems fail Commercial loss	✓	✓	×	✓	×	✓
A. Dardanelli, et al.[81]	2013	Bluetooth	Eavesdropping, Sniffing, Buffer-over-flow attack.	Vehicle systems fail Commercial loss	✓	✓	×	✓	×	×
Sudhir Pai, et al. [82]	2018	Remote key	Eavesdropping Sniffing, Buffering over-flow attack.	Vehicle systems fail Vehicle theft	×	×	×	✓	×	×

3.5 *Attacker type*

The Attacker or hacker of an autonomous system intention will vary on time and situation. The different types of hackers who host different threats to autonomous vehicles with different motives are elaborated in Table 7.

Table 7: Summary of sensor and actuator attacks in AGV

Hacker Type	Motive
Nation States	Steal the information to either control directly or to outsource the information
Criminal Gangs	To produce illicit income for the gangs using different schemes
Hacktivists	To create attention in the world by targeting highly visible or high-profile images
Cyberterrorists	To cause physical demolition of property or loss of life.
Insiders	Due to the reasons of money, philosophy, compulsion, self-esteem, vengeance, and politics, they do against the company or organization.
Unscrupulous Operators	To flunk the system, to get ahead in traffic, do competitor sabotage, etc.

4 Defense Mechanism and Countermeasures

In general, for conventional vehicles, the driver is responsible for all behavior of the vehicle. However, the autonomous driving system raises the questions against liability, "who is responsible for the autonomous vehicle which harms the people?" Hence it is essential to develop a model which prevents vulnerability inboth individual and interacting components of the automated vehicle. There are many defense systems wereproposed by various authors to handle various attacks. Safety and security are the two critical factors of therisk-free autonomous vehicle. In [82], the author proposed four strategies: Gateway Installation, EncryptionScheme, Authentication Mechanism, and Anomaly Detection. Three main phases are followed to handle the cyber-attacks in the autonomous vehicle, and they are (a) Attack detection, (b) Attack Prevention, (c) Recommendation system

4.1 Attack Detection Methods

Controller attack detection method - An intrusion Detection System [83] was proposed for in-vehicle network CAN. This method detects attacks like replay attacks, packet insertion attacks, and packet modification attacks. The detection approaches signature-based, anomaly-based (machine learning and statistical methods), and specification-based methods were deployed and validated. In [84], the detectionframework for CAN was presented with a rule-based approach and Recurrent Neural Network to detect DoS and replay attacks in the network. This method was tested with the accurate data of KIA Soul and Hyundai Sonata. To find the unauthenticated messages of ECU, the method of fingerprinting the messageswas implemented. This detection system was implemented, and the performance was evaluated[85]. In [86], the author detailed the hybrid anomaly detection mechanisms to detect and prevent cyber-attacks within ECUs. This approach is used to recognize unknown and newly arising cyber-attacks. This hybrid approach uses algorithms like Replicator Neural Networks (RNN), One-Class Support Vector Machines (OCSVM) and Lightweight Online Detector of Anomalies. Taylor et al. [51] proposed an anomaly detectorwith a Long-Short term memory recurrent neural network to recognize the malicious behavior of the CANnetwork. This approach detects five types of modification attacks: Interleave, drop, discontinuity, unusual,Reverse.

Sensor and actuator Attack detection method - For Sybil attack detection, In [87], the author analyzed the different Sybil attack scenarios in VANET and suggested three detection methods such as 1)resource testingmethods, 2) position verification 3)authentication based methods. The four-module-based detection systemwas recommended. The modules were Denoising, motion detection, static detection, dynamic detection. Moreover, the self-adaptive MUSIC algorithm was used [88]. Five detectors were introduced in [65] to findspoofing attacks in GPS using partial correlation spans time intervals. The performance of the detectors was evaluated. Robot intrusion detection systems (RIDS) were implemented with the Khepera mobile robotto detect actuator and sensor attacks[83].

Moreover, for GPS-based attacks, the detection mechanism with Receiver Autonomous Integrity Monitoring (RAIM) was used. This method was evaluated with different case scenarios [71]. Tuan [70] developed an intrusion detection system to deny service attacks in atomic vehicles using a decision tree algorithm. They have created the testbed, which is a four-wheel-drive robot. Eight different input features were collected at different locations with a specific period. Using a decision tree, the c5.0 algorithm is usedto detect the cyber-attack in the robotic vehicle. The set of rules accuracy is evaluated using the TPR (TruePositive Rate and FPR (False Positive Rate). Hence this model is only for DoS attack detection. The cyber-attacks onboard vehicle can be detected by using the intrusion detection approach module. The system is trained in offline mode to learn simple rules about its normal behavior otherwise by using the signatures of different kinds of known attacks based on different monitored features [70]. When in the actual operation of the vehicle, it would monitor these identified features and apply the simple rules, whichwould have a relatively low processing load. However, this approach can work well for simple and previously known attacks. An alternative approach, in which offloaded to a powerful external processing system such as a cloud infrastructure to run the intrusion detection process is used [89]. This can condensethe processing load on the actual vehicle. Furthermore, it can also allow leveraging much more complex intrusion detection techniques, for instance, involving simple deep learning methods[90]. *Physical plant attack detection method* - The active and passive algorithms were developed to detective invasive and non-invasive attacks on the physical plants in AGV [69]. In [91], the author developed deeplearning-based detection method for physical and cyber-attack in AGV. *Analysis of various attack*

methods - All attack detection methods were mentioned above primarily classified as Signature based and Anomaly-based detection techniques. Based on the review, the detectionframework should be good enough to find attacks in all three layers of AGV with both signatures-based and anomaly-based manner. The main concern of the detection framework is to improve the detection accuracy rate and reduce the latency. To achieve this in the generative adversarial network (GAN) based on a generator and discriminator system can be used [92] [93]. Table 8 provides a comparative analysis of attack detection methods.

Table 8: Comparative analysis of attack detection methods

Ref	Method			Component			Types of attacks		
	Signature based	Anomaly based	Layer – 1attack	Layer – 2attacks	Layer – 3 attacks	Jammingattack	Spoofing attack	Replay attack	DoS attack
Lokmanet etal., [83]	✓	✓	✓	-	-	-	-	✓	-
Tariq et al., [84]	-	✓	✓	-	-	-	-	✓	✓
Hafeez et al.,[85]	✓	-	✓	-	-	✓	-	-	-
Pouyan et al.,[87]	✓	-	-	✓	-	✓	✓	✓	-
Wang et al.,[88]	✓	-	-	✓	-	✓	-	-	-
Gonzalo et al., [65]	✓	-	-	✓	-	-	✓	-	-
Guo et al.,[83]	✓	-	-	✓	-	-	✓	✓	-
Javaid et al.,[71]	✓	-	-	✓	-	-	-	-	✓
Vuong et al., [71]	✓	-	-	✓	-	-	-	-	✓
Sommer et al [94]		✓	-	✓	-	-	✓	✓	-
Giraldo et al., [73]	✓	-	-	-	✓	✓	✓	-	-
Dutta et al.,[69]	-	-	-	-	✓	✓	✓	-	✓
Deng et al.,[91]	-	✓	-	✓	✓	✓	✓	✓	✓

4.2 Attack Prevention Method

Prevention methods for controller attacks - In [70], the Authors proposed an identification model for CAN(Controller Area Network) protocol attacks using fuzzy algorithm. The model is capable of detecting four types of attacks, namely DoS (Denial of Service), fuzzy, rpm, and gear attacks. They used fuzzy algorithmslike Fuzzy Rough NN, NN, Discernibility Classifier, and FURIA to find the presence of attacks. This modelis analyzed using the weka tool. However, the actual vehicle implementation is not done. Kyong-Tak Choand Kang G. Shin have developed a model to find the attacks on ECU (Electronic Control Unit) and the Voltage Based Attacker Identification Model [95]. By measuring the voltage of ECU, attack messages areidentified. They have conducted experiments with two actual vehicles (Honda Accord- 2013 model and Chevrolet Trax-2015 model). The lattice-Based Double-Authentication method was proposed against the vehicle network by Liu et al. [96].

Prevention methods for senor and actuator attacks - The double reservation attack prevention method is proposed as a valet parking scenario in [97], the privacy-preserving scheme with cryptographic techniqueswas implemented, and performance was analyzed. A two-factor authentication mechanism was implemented to prevent GPS Spoofing attacks [79]. In which RSA based digital signature was used. In [98] blockchain-based architecture was proposed to

prevent cyber-attacks in AGV. Even though this method's prediction rate is high, few challenges are there to incorporate blockchain security methods in anautonomous vehicle. The modified Kalman filter and Chi-squared detector were used to prevent DoS attacks in autonomous vehicles' sensors. Moreover, the method was demonstrated with a case study[99]. *Analysis of Prevention methods* - There are many security attack detections methods implemented for specific components with specific attacks and integrated components. However, only a few prevention methods were proposed by the researchers. Those are broadly classified as Cryptography based and Software architecture based prevention mechanisms [98]. It is essential to prevent the attack before it affects the AGV. The table 9 describes the different types of attacks and their prevention method.

Table 9: Types of attacks and prevention idea

Types of attack	Prevention	Consequence
Hardware Theft	Ensure that the vehicle hardware parts are safeguarded physically at all times.	Lost revenue, Reputation damage, Identity theft, Theft of ideas, plans or other intellectual property, Consumer mistrust, Market share loss, Shareholder wariness, Loss of data privacy,Car safety, User safety,Financial loss for the consumer
Insecure storage or transmission of sensitive information	Ensure that sensitive data rests encrypted during storage and transformation and sustain control over who has access to folders.	
hacking or leaking passwords	Practice only secure, cryptic passwords and use various passwords for diverse levels of confidentiality.	
Missing patches and updating software	Confirm that all systems within the network are regularly updated with the latest versions.	
Virus or Trojan or malware	Use premier antivirus and anti-malware software and ensure it is updated frequently.	
Insecure disposal or reuse of hardware or software	Securely delete or abolish sensitive files before the clearance or reuse of any hardware or software.	

4.2 Recommendation System

The data attack preventive measures are summarized in table 10. Which compares the various defense methods. Based on this comparison a CEP based recommendation system is proposed for Autonomous Ground Vehicle (AGV) to protect the transportation system.

Table 10: Various Defense methods

Defense Method	Attack Detection		Implementation Details	
	HA	LA	SB	TB
Fuzzy-rough nearest neighbor classification[100]	√	-	√	-
Viden : Voltage based fingerprinting [1 0 1]	√	-	-	√
Decision Tree-based Classification for injection attacks detection [70]	√	-	-	√
Cloud-based deep learning for attack detection [89]	√	-	-	√
CEP - Q-method for predictive analysis [1 0 2]	-	√	√	-
Rule-based classifiers for CEP [103]	-	√	√	-
Data mining based auto CEP [104]	-	√	√	-
(HA – High Accuracy, LL – Low Latency, SB – Simulation Based, TB - Testbed Based)				

CEP based recommendation system model contains four main layers such as
Layer 1 - Data acquirer Layer: The performance sensory data and safety sensory data are the two types of sensed data collected from the sensors of the system. This raw data is given as a input for layer 2.

Layer 2 - Event Prediction: Two main components are used in this layer. One is AI engine and another oneis CEP. AI Engine uses Machine learning algorithms to predict the events. The predicted event is given asinput for CEP tool. Complex Event Processing (CEP) is accepted as an essential real-time computing paradigm for analyzing continuous data streams [102]. The current CEP systems support analytics over high-velocity event data and data variety in diverse domains concepts present in IoT event streams. It analysis the over high volumes of real-time event streams, thus uniquely incorporating all three dimensionsof Big Data, namely volume, velocity and variety [105]. CEP system identifies and analyses cause-and- effect relationships among events in real-time, allowing personnel to proactively take practical actions in response to specific scenarios [106]. Then the appropriate security feature is added by analysis methods.

Layer 3 - Decider Layer: It contains the analysis methods which are majorly classified as diagnostic analysis,predictive analysis, and prescriptive analysis. The diagnostic analysis is the simplest form of analytics which uses the data visualization techniques like Histogram, Bar chart, Pie chart, Scatter plot, Treemap. It is used for understanding or identifying the hidden facts and trends in the data. Data are often withinstructured and unstructured. Predictive analysis is used to predict the probability of occurrence of a future event. The prescriptive analysis provides the optimal solution for a problem. It is used to assist the decision-maker in identifying the best action or optimal solution.

Layer 4: Proactive event Layer based on the input of the decider layer, the necessary proactive event is proposed in proactive event layer. This event is activated by actuator.

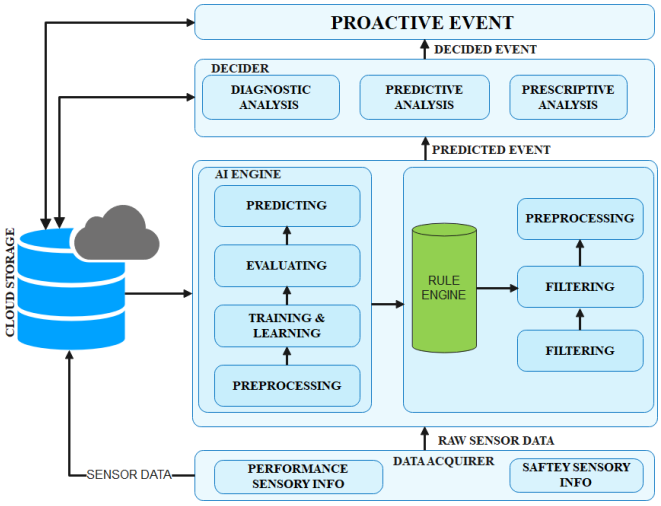


Figure 6: CEP based recommendation system for AGV

5 Discussions and Future directions

The security features in AGV in Cyber-Physical Systems will raise the following augmented questions tothe researchers.

- What are all the sensors needed for the AGV to optimize the prediction results?
- How can we upgrade security methods for detecting and predicting the vulnerabilities withoutaffecting the vehicle's performance?
- Which type of recommendation system can be provided after detecting vulnerability?Based on this review, answers are found.
- Depending on the purpose of the vehicles, advanced sensors can be identified, and practical sensorfusion

algorithms may be used.

- The security methods can have machine learning and deep learning algorithms with complex eventprocessing systems for managing performance for better prediction.
- After Detecting vulnerability, the system should alert the driver, and legitimate data should replacethe compromised data.

6 Conclusion

This survey provides a comprehensive understanding of the complexities and challenges associated with securing Autonomous Ground Vehicles (AGVs) integrated with Cyber-Physical Systems (CPS). By detailing the vulnerabilities and security methods of AGV systems, it offers valuable insights for researchers, developers, and policymakers working in the field of intelligent transportation systems. Readers will benefit from the detailed analysis of machine learning and deep learning algorithms in ITS, along with the review of security methods for overcoming threats in AGV systems. The comparison of different security approaches and their pros and cons aids in informed decision-making for securing AGVs. Furthermore, the proposed recommendation system, which utilizes machine learning algorithms in Complex Event Processing (CEP) for dynamic attack detection, presents a practical solution to enhance the security of intelligent transportation systems. Future research directions focusing on privacy-preserving recommendation systems will be crucial for ensuring the safety and security of AGVs in real-world deployments.

Statements and Declarations

Compliance with Ethical Standards

Disclosure of potential conflicts of interest

Funding

No funds, grants, or other support were received during the preparation of this manuscript.

Competing Interests

The authors have no relevant financial or non-financial interests to disclose

Data Availability

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Author Contributions

Two authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Dhivya Rathinasamy and Vishnu Kumar Kaliappan. The first draft of the manuscript was written by Dhivya Rathinasamy and the second author commented on previous versions of the manuscript. Both the authors read and approved the final manuscript.

References

1. Caporal JA, O'Neil W. Bridging the Divide: Autonomous Vehicles and the Automobile Industry. *Center for Strategic and International Studies (CSIS).* 2021.
2. Cupek R, et al. Autonomous Guided Vehicles for Smart Industries: The State-of-the-Art and Research Challenges. In: *International Conference on Computational Science.* 2020:330-343.
3. Parekh D, et al. A Review on Autonomous Vehicles: Progress, Methods and Challenges. *Electronics (Basel).* 2022;11(14):2162.
4. Ren K, Wang Q, Wang C, Qin Z, Lin X. The Security of Autonomous Driving: Threats, Defenses, and Future Directions. *Proc IEEE.* 2020;108(2):357-372.
5. Oyekanlu EA, et al. A Review of Recent Advances in Automated Guided Vehicle Technologies: Integration Challenges and Research Areas for 5G-Based Smart Manufacturing Applications. *IEEE Access.* 2020;8:202312-202353.
6. Yeong DJ, Velasco-Hernandez G, Barry J, Walsh J. Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review. *Sensors (Basel).* 2021;21(6):2140.

7. BloombergNEF. 9 of 10 Cars May Offer Advanced Safety Systems by 2030. *BloombergNEF.* 2020.
8. Golomb VM, Finkler L. State of the Advanced Mobility Industry 2021. *SAE International.* 2021.
9. Wunsch NG. Largest Patent Owners in Autonomous Driving Worldwide. *Statista.* 2021.
10. Rudolph G. Three Sensor Types Drive Autonomous Vehicles. *Sensors.* 2017.
11. Wang H, Zhang T, Zhang X. Observer-Based Path Tracking Controller Design for Autonomous Ground Vehicles with Input Saturation. *IEEE/CAA J Autom Sin.* 2023;10(3):749-761.
12. Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. Attacks on Self-Driving Cars and Their Countermeasures: A Survey. *IEEE Access.* 2020;8:207308-207342.
13. Mankodiya H, Jadav D, Gupta R, Tanwar S, Hong WC, Sharma R. OD-XAI: Explainable AI-Based Semantic Object Detection for Autonomous Vehicles. *Appl Sci.* 2022;12(11):5310.
14. Dixit P, Bhattacharya P, Tanwar S, Gupta R. Anomaly Detection in Autonomous Electric Vehicles Using AI Techniques: A Comprehensive Survey. *Expert Syst.* 2021.
15. Wiederer J, Bouazizi A, Troina M, Kressel U, Belagiannis V. Anomaly Detection in Multi-Agent Trajectories for Automated Driving. *CoRL.* 2021.
16. Boukerche A, Tao Y, Sun P. Artificial Intelligence-Based Vehicular Traffic Flow Prediction Methods for Supporting Intelligent Transportation Systems. *Comput Netw.* 2020;182:107484.
17. Ning H, Yin R, Ullah A, Shi F. A Survey on Hybrid Human-Artificial Intelligence for Autonomous Driving. *IEEE Trans Intell Transp Syst.* 2022;23(7):6011-6026.
18. He Y, Jolfaei A, Zheng X. Cyber-Physical Systems in Transportation. Springer; 2022.
19. Okafor KC, Ndinechi MC, Misra S. Cyber-Physical Network Architecture for Data Stream Provisioning in Complex Ecosystems. *Trans Emerg Telecommun Technol.* 2022;33(4).
20. Zinatullin L. Introduction to Information Security. In: *The Psychology of Information Security.* 2023:12-15.
21. Van Dijk L. Future Vehicle Networks and ECUs Architecture and Technology Considerations. *NXP Semiconductors.* 2017.
22. Checkoway S, et al. Experimental Security Analysis of a Modern Automobile. *IEEE Symp Secur Privacy.* 2012:1-16.
23. Buthker GS. Automated Vehicle Electronic Control Unit (ECU) Sensor Location Using Feature-Vector Based Comparisons. Wright State University; 2019.
24. Darr MJ, Stombaugh TS, Shearer SA. Controller Area Network Based Distributed Control for Autonomous Vehicles. *Trans ASAE.* 2005;48(2):479-490.
25. Yang JC, Lai CL, Sheu HT, Chen JJ. An Intelligent Automated Door Control System Based on a Smart Camera. *Sensors (Basel).* 2013;13(5):5923-5936.
26. Sviatov K, et al. Functional Model of a Self-Driving Car Control System. *Technologies.* 2021;9(4):100.
27. Pérez-Gil Ó, et al. Deep Reinforcement Learning Based Control for Autonomous Vehicles in CARLA. *Multimed Tools Appl.* 2022;81(3):3553-3576.
28. Biswas A, Wang HC. Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain. *Sensors (Basel).* 2023;23(4):1963.
29. Hang P, Chen X. Towards Autonomous Driving: Review and Perspectives on Configuration and Control of Four-Wheel Independent Drive/Steering Electric Vehicles. *Actuators.* 2021;10(8):184.
30. Ignatious HA, El Sayed H, Khan M. An Overview of Sensors in Autonomous Vehicles. *Procedia Comput Sci.* 2021;198:736-741.
31. Zhu L. Analyze the Advantages and Disadvantages of Different Sensors for Autonomous Vehicles. In: *Proc 7th Int Conf Social Sciences and Economic Development (ICSSED).* 2022:1020-1024.
32. Haris M, Glowacz A. Navigating an Automated Driving Vehicle via the Early Fusion of Multi-Modality. *Sensors (Basel).* 2022;22(4):1425.
33. Choi Y, Baek S, Kim C. Simulation of AEBS Applicability by Changing Radar Detection Angle. *Appl Sci.* 2021;11:2305.
34. Carpenter S. Autonomous Vehicle Radar: Improving Radar Performance with Simulation. *Ansys Advantage.* 2018;1:32-37.
35. Dai K, et al. LiDAR-Based Sensor Fusion SLAM and Localization for Autonomous Driving Vehicles in Complex

Scenarios. *J Imaging.* 2023;9(2):52.
36. Pidurkar A, Sadakale R, Prakash AK. Monocular Camera Based Computer Vision System for Cost Effective Autonomous Vehicle. In: *Proc 10th Int Conf Computing, Communication and Networking Technologies (ICCCNT).* 2019:1-5.
37. Naveen A, Bandaru N. Obstacle Detection Using Stereo Vision for Self-Driving Cars. In: *IEEE Intelligent Vehicles Symposium.* 2016:1-7.
38. Reid TGR, et al. Localization Requirements for Autonomous Vehicles. *arXiv.* 2019.
39. Butt FA, Chattha JN, Ahmad J, Zia MU, Rizwan M, Naqvi IH. On the Integration of Enabling Wireless Technologies and Sensor Fusion for Next-Generation Connected and Autonomous Vehicles. *IEEE Access.* 2022;10:14643-14668.
40. Hafeez F, Sheikh UU, Alkhaldi N, Al Garni HZ, Arfeen ZA, Khalid SA. Insights and Strategies for an Autonomous Vehicle with Sensor Fusion Innovation: A Fictional Outlook. *IEEE Access.* 2020;8:135162-135175.
41. Kim K, Kim JS, Jeong S, Park JH, Kim HK. Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Comput Secur.* 2021;103:102150.
42. Zhou X, et al. Strategic Safety-Critical Attacks Against an Advanced Driver Assistance System. In: *Proc 52nd IEEE/IFIP Int Conf Dependable Systems and Networks (DSN).* 2022:79-87.
43. Parkinson S, Ward P, Wilson K, Miller J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans Intell Transp Syst.* 2017;18(11):2898-2915.
44. Magazine S. Connected Vehicle Security Vulnerabilities. *IEEE Technol Soc Mag.* 2018:15-18.
45. Smith C. *The Car Hacker's Handbook: A Guide for the Penetration Tester.* San Francisco: No Starch Press; 2016.
46. Limbasiya T, Teng KZ, Chattopadhyay S, Zhou J. A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles. *Veh Commun.* 2022;37:100515.
47. Lin CW, Sangiovanni-Vincentelli A. Cyber-Security for the Controller Area Network (CAN) Communication Protocol. In: *ASE Int Conf Cyber Security.* 2012:1-7.
48. Bloom G. WeepingCAN: A Stealthy CAN Bus-Off Attack. In: *Workshop on Automotive and Autonomous Vehicle Security.* 2021.
49. Maggi F. A Vulnerability in Modern Automotive Standards and How We Exploited It. *TrendLabs Security Intelligence Blog.* 2017.
50. Buttigieg R, Farrugia M, Meli C. Security Issues in Controller Area Networks in Automobiles. In: *18th Int Conf Sciences and Techniques of Automatic Control and Computer Engineering (STA).* 2017:93-98.
51. Taylor A, Leblanc S, Japkowicz N. Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks. In: *IEEE Int Conf Data Science and Advanced Analytics (DSAA).* 2016:130-139.
52. Taylor A, Japkowicz N, Leblanc S. Frequency-Based Anomaly Detection for the Automotive CAN Bus. In: *World Congress on Industrial Control Systems Security (WCICSS).* 2015:45-49.
53. Tomlinson A, Bryans J, Shaikh SA, Kalutarage HK. Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows. In: *IEEE/IFIP Int Conf Dependable Systems and Networks Workshops (DSN-W).* 2018:231-238.
54. Wang C, Zhao Z, Gong L, Zhu L, Liu Z, Cheng X. A Distributed Anomaly Detection System for In-Vehicle Network Using HTM. *IEEE Access.* 2018;6:9091-9098.
55. Zhou A, Li Z, Shen Y. Anomaly Detection of CAN Bus Messages Using a Deep Neural Network for Autonomous Vehicles. *Appl Sci.* 2019.
56. Rizvi S, Willet J, Perino D, Marasco S, Condo C. A Threat to Vehicular Cyber Security and the Urgency for Correction. *Procedia Comput Sci.* 2017;114:100-105.
57. Dibaei M, et al. An Overview of Attacks and Defences on Intelligent Connected Vehicles. *arXiv.* 2019.
58. Hoppe T, Kiltz S, Dittmann J. Security Threats to Automotive CAN Networks: Practical Examples and Selected Short-Term Countermeasures. *Reliab Eng Syst Saf.* 2011;96(1):11-25.
59. Rastogi N, Rampazzi S, Clifford M, Heller M, Bishop M. Explaining RADAR Features for Detecting Spoofing Attacks in Connected Autonomous Vehicles. *arXiv.* 2020.
60. Raiyn J. Data and Cyber Security in Autonomous Vehicle Networks. *Transport Telecommun.* 2018;19(4):325-334.

61. Ayub MF, Ghawash F, Shabbir MA, Kamran M, Butt FA. Surveillance System Using Autonomous Vehicles. In: *IEEE Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS).* 2018:1-5.
62. He Q, Meng X, Qu R. Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles. *J Adv Transp.* 2020;2020:6873273.
63. Cao Y, Cyr B, Rampazzi S, Chen QA, Fu K, Mao ZM. Adversarial Sensor Attack on LiDAR-Based Perception in Autonomous Driving. In: *ACM Conf Computer and Communications Security (CCS).* 2019.
64. Petit J, Kargl F. Remote Attacks on Automated Vehicle Sensors: Experiments on Camera and LiDAR. In: *Black Hat Europe.* 2015.
65. Seco-Granados G, Gómez-Casco D. Detection of Replay Attacks to GNSS Based on Partial Correlations and Authentication Data Unpredictability. 2020.
66. Yeh ER, Bhat CR, Heath RW, Choi J, Prelcic NG. Security in Automotive Radar and Vehicular Networks. *Microwave J.* 2017;60(5):148-164.
67. Cui J, Liew LS, Sabaliauskaite G, Zhou F. A Review on Safety Failures, Security Attacks, and Available Countermeasures for Autonomous Vehicles. *Ad Hoc Netw.* 2019;90.
68. Chowdhury A, Karmakar G. Attacks on Self-Driving Cars and Their Countermeasures: A Survey. *IEEE Access.* 2020;8:207308-207342.
69. Dutta RG. Security of Autonomous Systems Under Physical Attacks: With Application to Self-Driving Cars. 2018.
70. Vuong TP, Loukas G, Gan D, Bezemskij A. Decision Tree-Based Detection of Denial of Service and Command Injection Attacks on Robotic Vehicles. In: *IEEE Int Workshop Information Forensics and Security (WIFS).* 2015:1-6.
71. Javaid AY, Jahan F, Sun W. Analysis of Global Positioning System-Based Attacks and a Novel Global Positioning System Spoofing Detection/Mitigation Algorithm for Unmanned Aerial Vehicle Simulation. *Simulation.* 2017;93(5):427-441.
72. Dash P, Pattabiraman K. Autonomous Cars: Past, Present and Future—A Review of the Developments in the Last Century, the Present Scenario and the Expected Future of Autonomous Vehicle Technology. In: *Workshop on Automotive and Autonomous Vehicle Security.* 2023.
73. Giraldo J, Sarkar E, Cardenas AA, Maniatakos M, Kantarcioglu M. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des Test.* 2017;34(4):7-17.
74. Shaaban AM, Chlup S, El-Araby N, Schmittner C. Towards Optimized Security Attributes for IoT Devices in Smart Agriculture Based on the IEC 62443 Security Standard. *Appl Sci.* 2022;12(11):5653.
75. Abdel Hakeem SA, Hussein HH, Kim H. Security Requirements and Challenges of 6G Technologies and Applications. *Sensors (Basel).* 2022;22(5):1969.
76. Guang X, Gao Y, Leung H, Liu P, Li G. An Autonomous Vehicle Navigation System Based on Inertial and Visual Sensors. *Sensors (Basel).* 2018;18(9):2952.
77. Francillon A, Danev B, Capkun S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In: *Network and Distributed System Security Symposium (NDSS).* 2011:431-439.
78. Kumar AD, Chebrolu KNR, Vinayakumar R, Soman KP. A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities. *arXiv.* 2018.
79. Siegwart R, Nourbakhsh IR, Scaramuzza D. *Introduction to Autonomous Mobile Robots.* 2nd ed. Cambridge, MA: MIT Press; 2011.
80. Giraldo J, et al. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput Surv.* 2018;51(4).
81. Dardanelli A, et al. A Security Layer for Smartphone-to-Vehicle Communication over Bluetooth. *IEEE Embed Syst Lett.* 2013;5(3):34-37.
82. Pai S, Hine R. Successful Execution of Remotely Piloted Autonomous Marine Vehicles to Conduct METOC and Turbidity Surveys. In: *IEEE/OES Autonomous Underwater Vehicles (AUV).* 2014:2-4.
83. Lokman SF, Othman AT, Abu-Bakar MH. Intrusion Detection System for Automotive Controller Area Network (CAN) Bus System: A Review. *EURASIP J Wirel Commun Netw.* 2019;2019(1):184.
84. Tariq S, Lee S, Kang H, Woo SS. CAN-ADF: The Controller Area Network Attack Detection Framework. *Comput Secur.* 2020;94:101857.

85. Hafeez A, Topolovec K, Awad S. ECU Fingerprinting Through Parametric Signal Modeling and Artificial Neural Networks for In-Vehicle Security Against Spoofing Attacks. In: *International Computer Engineering Conference (ICENCO).* 2019.
86. Weber M, et al. Embedded Hybrid Anomaly Detection for Automotive CAN Communication. In: *Embedded Real Time Software and Systems (ERTS²).* 2018.
87. Pouyan AA, Alimohammadi M. Sybil Attack Detection in Vehicular Networks. *Comput Sci Inf Technol.* 2014;2(4):197-202.
88. Wang C, Zhu L. Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information. *Sensors (Basel).* 2018;18(3):878.
89. Loukas G, Vuong T, Heartfield R, Sakellari G, Yoon Y, Gan D. Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning. *IEEE Access.* 2017;5:3491-3508.
90. Aldhyani THH, Alkahtani H. Attacks to Autonomous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors (Basel).* 2022;22(1):360.
91. Deng Y, Zhang T, Lou G, Zheng X, Jin J, Han QL. Deep Learning-Based Autonomous Driving Systems: A Survey of Attacks and Defenses. *IEEE Trans Ind Inform.* 2021.
92. Sedjelmaci H. Attacks Detection and Decision Framework Based on Generative Adversarial Network Approach: Case of Vehicular Edge Computing Network. *Trans Emerg Telecommun Technol.* 2020.
93. Kloukiniotis AMA, Papandreou A, Lalos A, Kapsalas P, Nguyen DV. Countering Adversarial Attacks on Autonomous Vehicles Using Denoising Techniques: A Review. *IEEE Open J Intell Transp Syst.* 2022;3:61-80.
94. Sommer F, Dürrwang J, Kriesten R. Survey and Classification of Automotive Security Attacks. *Information (Basel).* 2019;10(4):148.
95. Dibaei M, Zheng X, Jiang K, Abbas R, Liu S, Zhang Y. Attacks and Defences on Intelligent Connected Vehicles: A Survey. *Digit Commun Netw.* 2020;6(4):399-421.
96. Liu J, et al. Lattice-Based Double-Authentication-Preventing Ring Signature for Security and Privacy in Vehicular Ad Hoc Networks. *Tsinghua Sci Technol.* 2019;24(5):575-584.
97. Huang C, Lu R, Lin X, Shen X. Secure Automated Valet Parking: A Privacy-Preserving Reservation Scheme for Autonomous Vehicles. *IEEE Trans Veh Technol.* 2018;67(11):11169-11180.
98. Gupta R, Tanwar S, Kumar N, Tyagi S. Blockchain-Based Security Attack Resilience Schemes for Autonomous Vehicles in Industry 4.0: A Systematic Review. *Comput Electr Eng.* 2020;86:106717.
99. Dutta RG, Yu F, Zhang T, Hu Y, Jin Y. Security for Safety: A Path Toward Building Trusted Autonomous Vehicles. In: *IEEE/ACM International Conference on Computer-Aided Design (ICCAD).* 2018.
100. Martinelli F, Mercaldo V, Nardone V, Santone A. Car Hacking Identification Through Fuzzy Logic Algorithms. In: *IEEE International Conference on Fuzzy Systems.* 2017.
101. Cho KT, Shin KG. Viden: Attacker Identification on In-Vehicle Networks. In: *ACM Conference on Computer and Communications Security (CCS).* 2017:1109-1123.
102. Ziehn A, Markl V, Zeuch S. Complex Event Processing for the Internet of Things. *CEUR Workshop Proc.* 2020;2652:1-4.
103. Mehdiyev N, Krumeich J, Enke D, Werth D, Loos P. Determination of Rule Patterns in Complex Event Processing Using Machine Learning Techniques. *Procedia Comput Sci.* 2015;61:395-401.
104. Mousheimish R, Taher Y, Zeitouni K. Automatic Learning of Predictive CEP Rules: Bridging the Gap Between Data Mining and Complex Event Processing. In: *Proc 11th ACM International Conference on Distributed Event-Based Systems (DEBS).* 2017:158-169.
105. Zaffiro G, Marone G. Smart Mobility: New Roles for Telcos in the Emergence of Electric and Autonomous Vehicles. In: *AEIT International Conference of Electrical and Electronic Technologies for Automotive.* 2019:1-5.
106. Wang Y, Geng S, Li Q. Intelligent Transportation Control Based on Proactive Complex Event Processing. *MATEC Web Conf.* 2016;77:09004.