A Comprehensive Analysis of the Security of ML Integrated CPS as Autonomous Vehicles

[*1]Kesava Reddy Jangam, [2]R. Kumudham, [3]V. Rajendran, [4]C. Vinoth Kumar

[*1]Electronics and Communication Engineering, Vels Institute of Science Technology and Advanced Studies, Chennai, India.
[2]Electronics and Communication Engineering, Vels Institute of Science Technology and Advanced Studies, Chennai, India.
[3]Electronics and Communication Engineering, Vels Institute of Science Technology and Advanced Studies, Chennai, India.
[4]Electronics and Communication Engineering, Sri Sivasubramaniya Nadar College of Engineering, Chennai, India

[*]Corresponding author mail ID: kesava464@gmail.com

Abstract

Autonomous Vehicles (AVs) are the primary application in the context of Cyber-Physical Systems (CPS). The rapid advancement in the deployment of CPS within AVs have taken numerous of security challenges. Therefore, the CPS security model necessitates a significant instance of improvement in AVs field to assure a secure and reliable system. Moreover, the incorporation of Machine Learning (ML) techniques into CPS, which has effectively streamlined operations and reduced the complexity associated with AVs. This review paper aims to provide a comprehensive review of the security measures pertinent in CPS for AVs, specifically focusing on the integration of ML techniques within CPS. Moreover, the study discuss the impact of CPS in AVs, vulnerabilities detection in CPS with ML algorithm and benefits of CPS as a reusable module in terms of cost savings and development time. Furthermore, the paper surveys the crucial feature of risk assessment associated to autonomous vehicles, emphasising the performance can considerably improve when risk assessments are confirmed by large datasets in the training phase, predominantly while engaging learning models. Furthermore, it explores real-world Vehicle-to-Vehicle (V2V) communication applications, focusing on passenger safety and security enhancements. Overall, the findings emphasise the significance of leveraging progressive data analytics and advanced ML techniques to improve the security and reliability of autonomous vehicles with CPS, confirming the safe functions in progressively multifaceted atmospheres on road traffic.

Keywords: Cyber-Physical System, Machine Learning, Autonomous Vehicles

1. Introduction

Cyber-Physical System (CPS) is the interacting system that works together constantly with the human module and the physical, analog, and digital module. CPS integrates computational elements with physical processes, enabling real-time monitoring and control across various applications. In industrial settings, CPS enhances manufacturing automation, intelligent production lines, equipment monitoring, and the creation of digital twins, driving efficiency and predictive maintenance. Similarly in autonomous vehicles field, CPS employs sensors for data collection, a central controller for decision-making using AI, and actuators for executing driving commands, facilitating safe navigation. The deployment of physical and computational processes along with the sensors makes the CPS interact more efficiently (Ding et al., 2018). The CPS is responsible for monitoring the physical module with the received feedback from the digital module and controls it. The convergence of sensors, actuators, and controllers in CPS introduces unique challenges such as span real-time operation, safety, security, and overall system robustness, necessitating advanced solutions for managing complex interactions due to the intricate integration of physical and computational elements. Addressing issues such as network delays, cyber security threats, and sensor-actuator coordination is crucial for ensuring reliable and efficient CPS performance.

The application of CPS is already evident in fields such as healthcare, transportation, and aerospace, where their use is particularly prevalent in applications that demand maximum reliability and security against adversarial attacks. However, CPS security is essential for safeguarding the integrity of operations that intertwine digital and physical systems. The rapid mark-up in the security methods has paved the way for the emergence of smart security through

CPS. Thus, the CPS security model along with the Machine Learning (ML) has raised and reliability in ML techniques can be obtained by deploying trained samples that may not available for certain features (Olowononi et al., 2020).

However, the desired design of CPS security model with required specifications is not possible always as CPS is intended to function under undefined scenarios. To combat this, CPSs are integrated with the ML techniques that are driven by data. For the control of autonomous vehicles in the mapping of images, Convolutional Neural Networks (CNNs) are employed in certain critical tasks like adversarial attacks (Harrison et al., 2024). Moreover, deployment of ML methods into the CPS can at times cause three types of impacts, one is the good impact where prolific benefits are obtained as a result of using ML with the CPS. The next is the bad impact where the ML techniques are attacked with a misleading process of training. The third is the ugly impact where ML is used to attack the CPS security model. These impacts can be avoided by restraining the ML capabilities, by pre-testing the ML techniques in the environments that are simulated and lastly, a fortified framework can combat the attacks (Liang et al., 2019). ML techniques are commonly employed along with CPS in autonomous vehicle systems where Deep Neural Networks (DNNs) are used to identify the adversarial attacks and the control the security system. But still, risk calculation remains as false signals are critical in such methods (Pereira & Thomas, 2020).

The rapid development of communication technology with smart based transportation systems have obtained numerous attention from various organizations. However, the recommended research (Feng et al., 2018) have concentrated in the systematic methodologies which existing researches have explored as a limitation. It has used a distributed based CPS for both forms of automated and connected system vehicles related techniques have been utilized. Each kind of vehicle in the particular system has been modeled with the double level integrator and allowed for travelling along the path of trajectory in order to maintain rigid formation. The desired level of trajectory has been generated through reference obtained from leading systems with the utilization of data from various sources and the normal vehicles follow using position and velocity related data from the closest neighbours and sensor data from the on boarding sensors have helped in managing the performance. Information-graphs have been used for depicting the topology of interaction between vehicles. Edge based computing have been used for analysis with the processed information such as for minimizing the risk in data leaks. Performance has been scaled from single dimensional graph to multi-dimensional data graphs. The experimental predictions have revealed better performance. The suggested research (Lv et al., 2018) has focused on the codesign based optimization strategy for determining the level of optimal adaptation to automatically control balancing of intelligent vehicle systems. The CPS security model utilized for the optimization of control parameters for the automatic vehicle with respect to varying performance of vehicle with energy and drivability factors with different styles. It also has performed investigation on requirements and system methodologies and utilized the driving-style-recognition approach with the assistance of unsupervised ML and has been validated with various experiments. The adaptive-controlling method has been designed with three different styles of driving with various protocols. The exploration has been made on performance with parameter level optimizations have been implemented with objective criteria. The evaluations from the automated vehicle have shown that the controller have performed effective on all tasks under moderate, aggressive and conservative styles of driving. The validated outcomes have proved the efficiency and feasibility of the system. However, a safer autonomous vehicular system with the CPS security model thrusts the challenges as the operation of the autonomous system is not fixed to a particular environment. Hence the design of such systems must consider an unexpected environment with faults along with the expected operating environment. In addition to that, a complete autonomous CPS can be designed by considering the unexpected conditions in the urban landscapes, providing manned vision like sights in such vehicles. The present paper enumerates the systematic review of the present studies of the security of autonomous vehicles with CPS along with the ML techniques. The major contribution of the study involves,

- To describe core components in CPS and the factors that influence CPS performance in terms of security is analysed that assist to design the most secure and reliable CPS security model
- To exhibit the various reviews of deployment of ML- Machine learning techniques for effective CPS.
- To analyse the various security threats, risk assessment associated with the implementation of ML integrated CPS for autonomous vehicles.
- To explore real world application with V2V communication to ensure safe and security of the passenger

Paper Organisation

This paper is organized in the following way. Section I enumerates the introductory section of the review. The next section II elaborates on the Cyber-Physical System with the Machine Learning techniques and the security associated

with them. Section III briefly explains the security threats of autonomous vehicles and the risk assessment methods followed by them. The last section IV is the conclusion part of the work.

2. Cyber-Physical System

In this section, the CPS key components, security issues, vulnerabilities detection with ML techniques, The impact of CPS for AVs and benefits of CPS as a reusable model in the autonomous vehicles are discussed.

2.1 Core components in CPS

According to a source, CPS is described as a network system that includes cyber (communication and computation) and physical (actuators and sensors) components interacting in a feedback loop with potential human intervention. In these systems, data is collected through physical components and transferred to the cyber component with minimal human involvement. The physical devices commonly used are infrared sensors, RFID tags, or barcodes (Agrawal & Kumar, 2022). CPS is utilized across different sectors such as manufacturing, energy, infrastructure, consumer goods, military, robots, smart buildings, communications, healthcare, and transportation. Both automation and self-optimization techniques are implemented to improve processes. CPS integrates computing, storage, and communication functionalities with the monitoring and management of physical components. Essentially, physical objects are endowed with "intelligence" to enable communication among themselves. Due to their interconnected nature, they leverage global digital networks to monitor, control, and utilize information in the virtual realm, enabling learning, cooperation, and evolution. The figure 1 depicts the key elements in CPS.

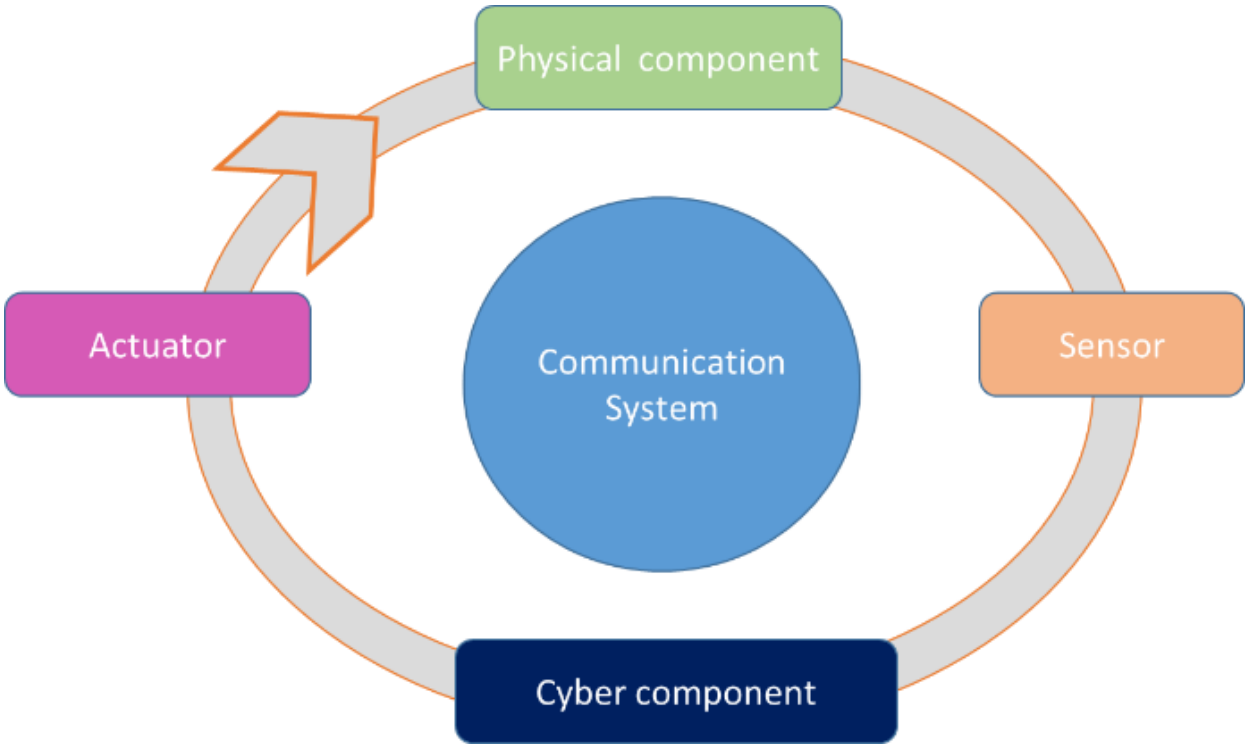

Figure 1 Core components in CPS

The implementation of CPS in autonomous vehicles is significantly influenced by several critical factors, including sensor noise, communication latency, and hardware limitations. AVs relay on sensors such as LiDAR, radar, and cameras to perceive their environment. However, these sensors can be adversely affected by environmental conditions, leading to noise that can compromise data accuracy. For instance, adverse weather like rain can obscure sensor readings. Likely, communication latency can hinder decision-making processes, particularly in dynamic scenarios where rapid responses are critical for safety. Delays in data transmission can result in outdated information being used for navigation and obstacle avoidance, increasing the risk of accidents. Additionally, hardware limitations, including the high cost and complexity of necessary components, complicate the deployment of these systems. The intricate nature of advanced hardware can also lead to maintenance challenges and increased operational costs due to potential failures. Addressing these factors is crucial for enhancing the reliability and safety of autonomous vehicles. Continuous technological advancements are required to minimize sensor noise, reduce communication delays, and

improve hardware affordability. By overcoming these challenges, the potential of CPS in autonomous driving can be fully realized.

Moreover, to ensure long-term reliability in AVs, particularly regarding wear and tear on physical components and the degradation of ML model performance can be resolved by holistic CPS architecture that integrates safety assurance and performance improvement is essential. This includes creating probabilistic algorithms that provide collision avoidance guarantees under rare events, thus enhancing reliability over time.

2.2 CPS security model

The recent developments of CPS as smart structures, devices, robots for industrial applications, and autonomous vehicles have been so incredible. Amidst the rapid development of such systems, certain challenges result out of intricacy in the functionality of the system. The specific requirement of the system with safety and security along with high withstanding capacity under erroneous situations makes the complexity much higher. Hence, error-free autonomous behaviour of the system can be obtained if the design engineers consider broader design criteria with specific requirements even under unexpected conditions (Zhu et al., 2018). Security and safety are often vulnerable as the specific requirements of the connections that are present within the system and the actuators, controllers, sensors create more chances of attack (Olowononi et al., 2020). The intrinsic behaviour of the CPS is the interconnections of the components and the regular connection with the physical environment and the human module makes the efficiency of the systems to be used for autonomous conditions. Moreover, these integrations require synchronization and mutual aid for interconnectivity to be efficient (Fei et al., 2019).

The CPS design is mainly composed of the physical components or the hardware components along with power and energy administration. These physical components also encompass the respective network configurations with better availability. In addition, CPS also constitutes the spatial and temporal scale that satisfies the time constraints and proper detection with the autonomous condition. The fundamental of the CPS is its system that contains the information where they are used for the specific requirement along with the software modules. In other words, CPSs are the systems that are diversified with deeper interconnections and acquire information from the systems. These integrations are responsible for handling the time specifications and locations. The main criteria required for any CPS are proper detection, user-specified requirements with real-time applications, and security. Since the network and physical region of CPS are exposed the chances of intrusion, attacks, etc. are high. Hence CPS is intended to be more precautious in dealing with such attacks and mishaps. The complexities inherent in CPS significantly influence their design and functionality, particularly regarding safety and security requirements. CPSs are characterized by heterogeneity, involving diverse components that interact across various domains, which complicates their development and integration. This heterogeneity leads to challenges in managing multiple properties, behaviors, and performance targets, necessitating robust methodologies to address the resulting complexity. Furthermore, the dynamic nature of CPSs introduces unpredictability in system behavior, making it difficult to foresee potential failures or security breaches. The increasing openness of these systems expands their attack surfaces, heightening security risks that must be managed proactively. Additionally, the integration of AI within CPSs adds layers of complexity, as the robustness of AI algorithms is not fully understood, impacting safety outcomes. Effective design necessitates a comprehensive understanding of these complexities and the implementation of strategies that ensure both safety and security throughout the system's lifecycle. For any CPS to be efficient that should be more secured, credible, predictable, dynamic and end to end applicable in a real scenario. If these requirements are satisfied then falsified detection will not occur and action in an unexpected environment will be done without hindrance (Mishra et al., 2023).

To address the increasing complexity of CPS and guarantee flawless autonomous behaviour, design engineers have various methods at their disposal. Employed component-based design approaches and Pre-Integrated Architectures (PIARCHs) (Gougeon & Hamelin, 2023) could help reduce complexity and decrease research and development efforts. Complexity metrics play a crucial role in assessing the impact of PIARCHs, demonstrating their advantages in both theoretical and practical scenarios. Model-based and computer-aided engineering are indispensable tools, and design methodologies need to take into account interconnected factors (Arrieta et al., 2024). Implementing self-adaptive software models can support DevOps for intelligent CPS, extending to the embedded system level. Digital Twins (Acharya, 2024 #38) incorporated into software systems to offer a real-time representation of the CPS operational environment, facilitating autonomous decision-making. Utilizing Integrated Formal Methods in the CPS design process can guarantee that specified functional and non-functional requirements are fulfilled. Furthermore, integrating cyberattack detection and tolerance strategies into the design process can enhance the resilience of CPS. CPS security models are at risk of being targeted by cyber threats and adversarial attack, highlighting the need for robust resilience plans to guarantee their ongoing operation and successful recovery. Cyber-physical resilience refers

to the ability of an interconnected system to remain operational, even if certain functions are compromised. A comprehensive strategy is essential to safeguard CPSs from cyber-attacks like adversarial attack, incorporating measures like secure design, risk evaluation, surveillance and reaction, redundancy and backup systems, and training and education. Such proper and falsified detection can be seen in figure 1.

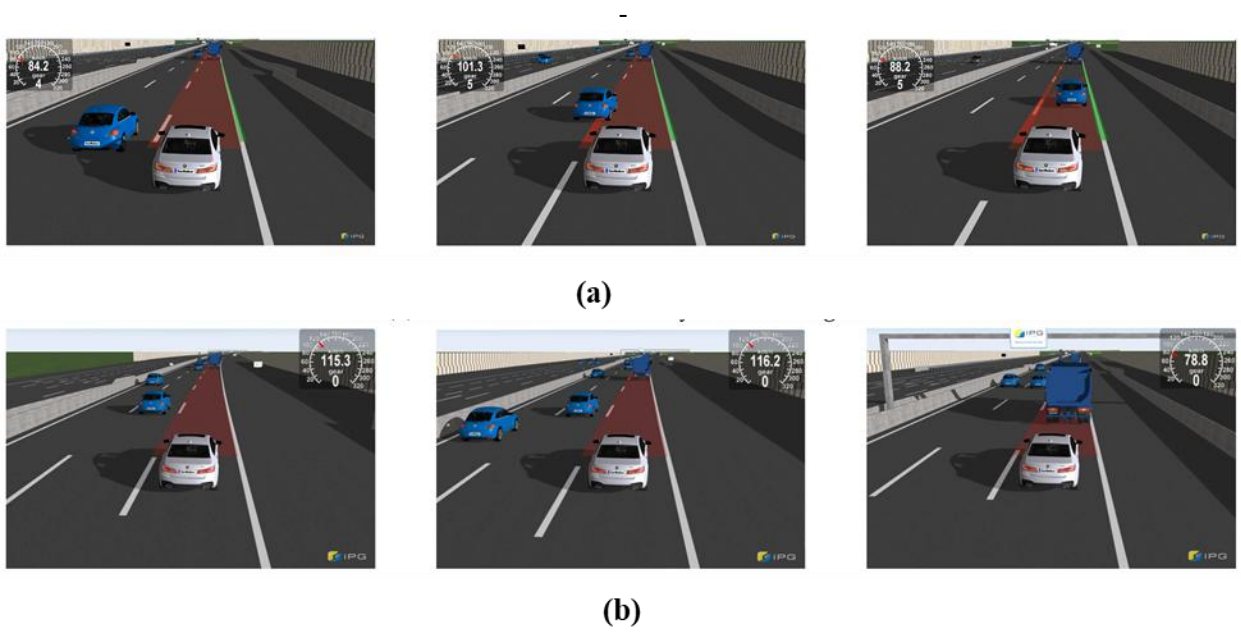

Figure 1 Autonomous Vehicles Detection (A) Lane Change (B) Speed Reduction (Nalic et al., 2020)

One more attribute to be considered in the security of CPS design is the prior deployment of evaluation and testing in the earlier stages than testing in the final phase. Most of the failures of the CPS are due to the testing them in the final phase than considering testing in the earlier stage where the failure of small peripherals can be identified better (Anumba & Roofigari-Esfahan, 2020). Implementing rigorous adversarial testing and validation processes significantly enhance the safety and security of CPS by systematically identifying vulnerabilities and ensuring compliance with operational requirements. These processes involve techniques such as formal verification, simulation-based testing (Birchler, 2024 #62), and runtime verification, which help detect potential failures and assess the system's resilience against cyber threats. By implementing these strategies throughout the development lifecycle, organizations can ensure that CPS operate reliably in real-world scenarios. Additionally, cyber-physical testbeds allow for realistic evaluations of system behavior under various conditions, improving operator training and developing robust defense mechanisms. Overall, these rigorous V2V processes are critical for minimizing risks and ensuring the safe deployment of CPS in diverse applications.

2.3 Machine Learning in CPS

Machine Learning (ML) techniques are mostly employed in the systems that are integrated with the human module in the environment that is shared. Integration of ML along with CPS security model is on the go in recent years for the critical safety of autonomous vehicles whose contribution can be seen in figure 2. ML techniques are deployed as certain applications cannot be handled with non-conventional methods. Hence ML safety features are concentrated more to increase the operability of the integrated system under unexpected conditions.

The safety of the ML integrated CPS security model can be obtained by identifying and analyzing the safety risks associated with the ML techniques. With the analysis and identification of the risks associated with the ML, proper design of the integration with CPS for autonomous vehicles can be achieved by avoiding the criticalities in the system (Pereira & Thomas, 2020). Generally, the output of ML depends upon the input as the specifications are transferred in the basic stages. However, the ML technique has plunged researchers to focus more as the need for them in the CPS integration for autonomy is increasing (Nagar et al., 2021).

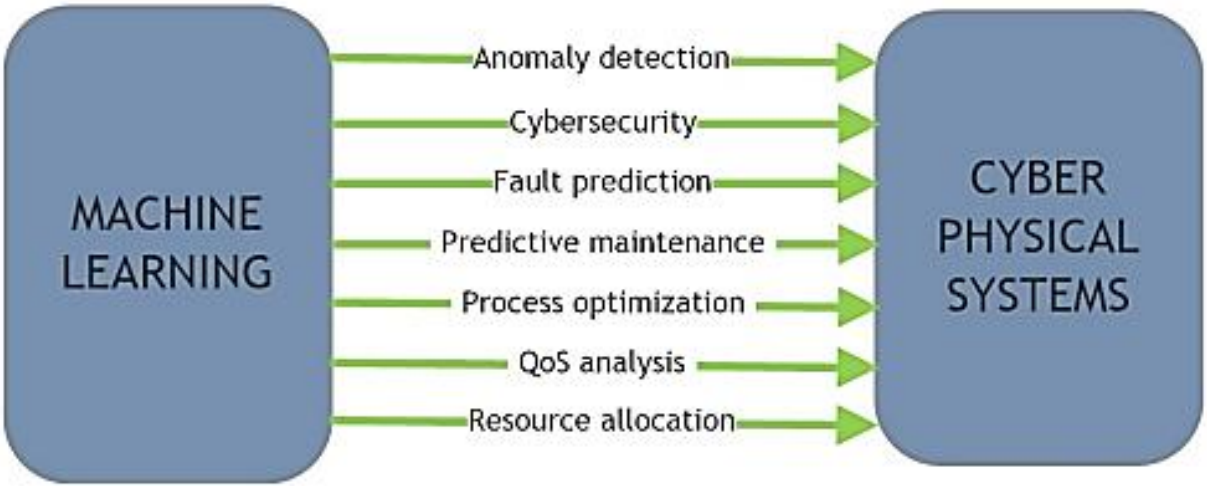

Figure 2 Machine Learning Technique for CPS (Olowononi et al., 2020)

The critical safety of the CPS has gained security and reliability threats with the integration of the internet of things. This is mainly due to the complexity of the CPS and the depending vulnerability due to the rising issues with the safety of the system. Hence an approach to the safety threat is elaborated in (Sheikh et al., 2022) where the security and reliability of the system are considered in identifying the failure in the operation and design time. As the complexity of the system rapidly marks up, ML integrated with CPS and the internet of things finds more reliable in the autonomous vehicle.

Moreover, falsification in CPS involves validating that the system adheres to specified temporal logic properties. This is crucial because ML components can produce outputs that lead to system failures under certain conditions. A compositional framework for falsification has been proposed that integrates temporal logic falsifiers with ML analyzers to identify inputs that violate system specifications. For instance, in an Automatic Emergency Braking System (AEBS), the system must accurately detect obstacles to prevent collisions. A structure for the detection of falsified signals with the ML component will suffice in finding the false signals. The falsified prediction is shown to be implemented with the deep neural network (DNN). The falsified signals are identified with wrongly identified features provided by the ML analyzer and classifier. The results of such methods are shown to be implemented in autonomous transportation (Pereira & Thomas, 2020). As the need for the security of the CPS is rising, various studies show that the data science outlook can be a suitable remedy for the security of CPS. The analysis of security-related issues previewed also suggests that ML can combat the threats to security from attacks (Jamal et al., 2021). Likewise, DNNs play a crucial role in enhancing the security of AVs through various mechanisms like anomaly detection, Instrusion Detection System (IDS) and data integrity verification. Various ML techniques for CPS are presented in table 1.

Table 1 Comparative Analysis of ML Techniques for CPS

S.No	Method	Dataset Description	Advantages	Disadvantages	Ref
1.	EPIC Electrical Power and Intelligent Control	CPS Electric power dataset	Use of operational testbed permits realistic simulations and provide valued description for potential vulnerabilities.	The study mainaly focus on the particular attack and affcets the smart grid systems.	(Adepu et al., 2020)
2.	First-Difference Aware Machine Learning classifier using Artificial Neural Network	New York Independent System Operator dataset	The structure can adapt to various network dimensions and complexity and utilize effective resource.	Inadequate data can be resultant in the lower prediction	(Aziz et al., 2023)

3.	Detection of anomaly through unsupervised ML	Secure Water Treatment (SWaT) dataset	The model can handle irregular training data effectively and applicable for real-time implementations	There exist complexity in implementation because it has to be tuned with care.	(Xi et al., 2022)
4.	ARC-Autonomous Response Controller	The industrial dataset collected from cyber attacks	Proactive threats are mitigated during real-time monitoring.	The model aims to lower the false positives and incoparate AI and it leads to misclassification	(Catillo et al., 2023)
5.	The method based on Hybrid Automaton	Data from CSTR-Continuous Stirred Tank Reactor test-bed	It DRL-IRS agent can learn different CPS environments with real-time response	The inconsistencies among the simulation and real-time CPS that leads to the suboptimal efficiency.	(Bashendy et al.)
6.	MAS-Multi-Agent System with BPNN- Back Propagation Neural Network	Industrial data from the construction field	Strong and efficient security for CPS	Improvements are required in the system through advanced research	(Lv et al., 2021)
7.	A fault detection system that is based on neural networks	Dataset collected from vehicular CPS	The structure allows to scale effortlessly with the addition of sensors deprived of substantial re-design	Complexity may arise due to distributed structure. Besides, there may be delay due to locality processing.	(Ruan et al., 2022)
8.	CRN attacks on the physical layer are reviewed	As it is reviewed no data set is required	Various attacks are elaborated	The empirical analysis is not available	(Salahdine & Kaabouch, 2020)
9.	Detection of the anomaly with random forest and k nearest neighbor	Data collected from cyber production systems	The structure can be easily scaled to provide wide-range of network and so it mitigate the impact of CPPS and improves detection accuracy.	It has the complexity with implementation of DDoS attack detection.	(Saghezchi et al., 2022)

2.5 The impact of CPS for Autonomous Vehicle

CPS combine computational components with physical operations, utilizing algorithms and real-time data analysis to oversee and manage physical operations. Likely, Autonomous vehicles (AVs) are a prime example of CPS, relying on sensors, cameras, and software to navigate and make decisions independently. CPS in autonomous vehicles rely heavily on connectivity for real-time data exchange. This connectivity enables efficient Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, enhancing safety and traffic management. Secure network architectures like 5G are crucial for handling high-bandwidth data transmission with low latency. By integrating robust connectivity, CPS designs can significantly improve the performance of autonomous vehicles within smart city environments. Thus, AV with CPS are equipped by sensors, actuators, and controllers that communicate to adjust the vehicle's speed and position. However, AV with CPS are susceptible to cyber-attacks that could disrupt transportation systems and lead to accidents particularly in urban environments. To address these vulnerabilities, research is focused on creating intelligent intrusion detection systems using CNN models to strengthen the security of AV networks.

Accordingly, the study (Alsulami et al., 2023) has employed transfer learning to identify cyber-attacks targeting connected physical components via network infrastructure for autonomous vehicle cyber-physical systems. It has developed controller area network (CAN) and integrating it into an AV simulation model, generated a dataset from the AV-CPS, pre-processed the dataset, and trained and tested it using pre-trained CNNs. Findings have revealed that GoogLeNet outperformed other pre-trained networks, achieved an F1-score of 99.47% in identifying cyber-attacks. Another study (Guo et al., 2022)developed address the path tracking control problem of autonomous vehicles (AVs) under cyber-attacks within a CPS framework. The methodology involved establishing nonlinear state and measurement equations of AVs under cyber-attacks based on a vehicle dynamics model, introducing sensor redundancy to improve robustness, and designing a cyber-attack detection method using an extended Kalman filter (EKF). The simulation results have demonstrated the effectiveness of the proposed control strategy. Likewise, in study (Pundir et al., 2022) aimed to understand smart CPS enabled with transportation systems, including its conceptual framework, connected and automated vehicles, associated technologies, and communication networks. It explores the expected demands of the transportation domain in future smart cities and the capabilities of CPS in a demand-supply framework. It analysed the high heterogeneity and complexity of CPS, which made the transportation domain susceptible to cyber vulnerabilities, and discusses designing, developing, and deploying models and algorithms to harness the powers of the integrated CPS system.

2.6 Vulnerabilities detection in CPS using ML models

CPS security model integrate computational elements with physical processes, making them susceptible to various vulnerabilities that can lead to severe consequences, particularly in critical infrastructures. Thus, that could be identified in order to improve the model reliability and scalability. Accordingly, the study (Bharathi, 2024) has implemented to enhance the cyber security in the CPS system by employing various ML models such as Decision Tree (DT), Random Forest (RF), and Ensemble crossover XG boost classifier. The outcome has revealed that XG boost classifier yielded the highest accuracy. Another study (Dhiman et al., 2021) has employed various ML techniques focusing on classification methods for threat monitoring and mitigation. The dataset utilized included real-world scenarios from healthcare and autonomous vehicles to evaluate the effectiveness of these algorithms. Results indicated significant improvements in detecting vulnerabilities and mitigating threats, demonstrating the potential of ML in securing CPS architectures. Recommendations were provided for model selection and training processes to optimize future applications in this domain. Likewise, in study (Pavithra et al., 2023) focused to enhance the security of Intelligent Transport Systems (ITS) by addressing vulnerabilities and countermeasures from a cyber-physical systems perspective. It has utilized a reinforcement learning algorithm to develop adaptive security measures capable of learning from interactions within the ITS environment. The dataset comprised simulated attack scenarios and real-time traffic data to train the RL agent effectively. The obtained results demonstrated that the RL-based approach significantly improved the detection and response to cyber threats, showcasing its potential in real-world applications of ITS security. Overall, the findings indicated that integrating RL could lead to more resilient and intelligent transportation networks.

Moreover, to strengthen the resilience of CPSs against cyber-attacks employed strategies like enhanced system design, effective monitoring and data analysis automated recovery system and robust communication protocols. By implementing these strategies, organizations can significantly enhance the resilience of CPS against cyber threats, ensuring their reliability and security in critical infrastructure contexts.

2.7 Benefits of CPS as reusable modules in the Automation of Vehicle systems

CPS offer several benefits when used as reusable modules in the AVs, particularly in terms of cost savings and development time. Reusability reduces redundant development and maintenance efforts, leading to cost savings and accelerating the overall time to market for software products. It enhance vehicle automation by promoting modularity, which allows for the reuse of components across different applications. This leads to improved efficiency, reduced development time, and easier integration of new features while ensuring safety and reliability in vehicle systems.

Consequently, the existing study (Meng et al., 2023) has developed an integrated design framework for the perception system of automated electric vehicles, focusing on optimizing sensor reusability to reduce costs and enhance hardware efficiency. The methodology employed a feature-oriented distributed design approach based on swarm intelligence optimization, generating multiple design schemes that balance performance and cost, supported by fuzzy reasoning for scheme selection. The results have demonstrated the framework's effectiveness through a simulation case study,

validating its ability to produce comprehensive design schemes while improving sensor utilization. Similarly in study (Neema et al., 2023) focused to establish reusable and configurable network simulation component for CPS co-simulations, addressing the challenges of integrating various physical domains and network characteristics that influence CPS performance. The methodology has included creating a cyber-attack library to analyze CPS behavior under attack conditions, facilitating the exploration of cyber scenarios through networked co-simulations. Results indicated that this approach can significantly enhance the effectiveness and efficiency of CPS simulations, enabling better preparedness against cyber threats in diverse application domains. Likewise, in study (Hoepfner et al., 2023) tackled the integration challenges of physical and mechanical behavior within Model-Based Systems Engineering (MBSE) for CPS. It employed a model-based methodology that incorporated detailed physical effects into the MBSE framework, facilitating a comprehensive virtual development process. The methodology was evaluated using a real automotive use case, demonstrating enhanced virtual development capabilities and potential for automated development and continuous integration across various domain and emphasized the cost savings and development time.

3. Security in Autonomous Vehicles

The invention of Autonomous vehicles (AVs) has provided many benefits that increased safety and minimized the energy consumption, congestion, that are the typical representation of the CPS . The vehicles gather information from the physical module through components like actuators, and sensors and examine the obtained real scenario information with the application-specific devices. From this, these devices are responsible for deciding and controlling the hardware and the components. However, the convergence of sensors, actuators, and controllers in CPS introduces unique challenges such as span real-time operation, safety, security, and overall system robustness, necessitating advanced solutions for managing complex interactions due to the intricate integration of physical and computational elements. Addressing issues such as network delays, cyber-security threats, and sensor-actuator coordination is crucial for ensuring reliable and efficient CPS performance with autonomous vehicle.

Consequently, the conventional study (Sun et al., 2023) has implemented to address the secure event-triggered path following control problem for autonomous vehicles facing sensor and actuator attacks like adversarial attacks. It utilized a feedback linearization method based on Lie derivative to transform a nonlinear attacked model into a linear form, facilitating further analysis and design. The dataset involved simulations and experimental setups that tested the control scheme against various attack scenarios. Results demonstrated that the proposed secure sliding control effectively mitigated the impacts of false data injection attacks while maintaining the original control structure. Formal stability criteria and controller design were expressed through linear matrix inequalities, confirming the robustness of the approach. Similarly, the existing research (Bendiab et al., 2023) has focused to enhance the security and privacy of autonomous vehicles (AVs). It has employed a hybrid algorithm that synergized AI-driven anomaly detection with Blockchain's immutable ledger capabilities. The researchers utilized datasets comprising simulated AV sensor data to evaluate the effectiveness of their proposed solutions. The findings have indicated significant improvements in threat detection and data integrity, demonstrating the potential of this amalgamation to address critical security vulnerabilities in AV systems. Likewise, in study (Aldhyani & Alkahtani, 2022) created a system that uses AI techniques to protect AV networks from cyber threats. It has employed DL based models such as CNN and hybrid CNN-long short-term memory (CNN-LSTM) models to identify attack messages. The system was tested using a real autonomous vehicle network dataset that included spoofing, flood, and replaying attacks, achieving a high accuracy of 97.30% in detecting and classifying these attacks.

V2V (Vehicle-to-Vehicle) and V2X (Vehicle-to-Everything) protocols are crucial for enhancing road safety and traffic efficiency. They enable real-time communication between vehicles and their surroundings, helping to prevent accidents, optimize traffic flow, and support the development of autonomous driving technologies. Therefore, the prior study (AlEisa et al., 2023) aimed to enhance the security of Intelligent Cyber-Physical Transportation Systems (ICTS) by developing a DL-based Intrusion Detection System (IDS) for monitoring In-Vehicle Networks (IVN), V2V, and Vehicle-to-Infrastructure (V2I) communications. It has utilized an ensemble LSTM algorithm to detect malicious activities within autonomous vehicle networks. Two datasets were employed for evaluation namely the car hacking dataset for internal vehicle communications and the UNSWNB15 dataset for external communications. Experimental results have indicated that the developed IDS significantly outperformed existing solutions in terms of detection accuracy and efficiency. This advancement suggested a promising direction for improving cyber security in smart transportation systems.

3.1 Risk assessments in Autonomous Vehicles

Typically, the autonomous vehicles with cyber systems are more complex and integrated than the conventional vehicles as they have the access and capability in communicating with the physical module. There are certain risk management schemes for the security of autonomous vehicles, one among them is the autonomous Supervision and Control System (SCS). These systems are generally based on CPS that are autonomous. This helps in the reduction of chances of failure through the collapse of the system for which an irrepressible sequence of actions is employed. In addition to that warnings are provided based on the zone of the incident which is the incident zone warning and can be seen in figure 3. This further enables providing temporal and spatial alertness which reduces the collapse of the system. This also helps in the detection of hazards in autonomous vehicles (Conrad et al., 2023).

The design optimization of electric vehicles such as CPS also provides an automated system. For such design, the requirements, optimizations, etc. are considered in the design of the vehicles. Unsupervised ML is employed in the recognition of the driving style. These techniques are also validated manually. Results indicated that autonomous vehicles with such an optimization outperformed under hostile, medium, and conventional styles of driving (Khanfar et al., 2022).

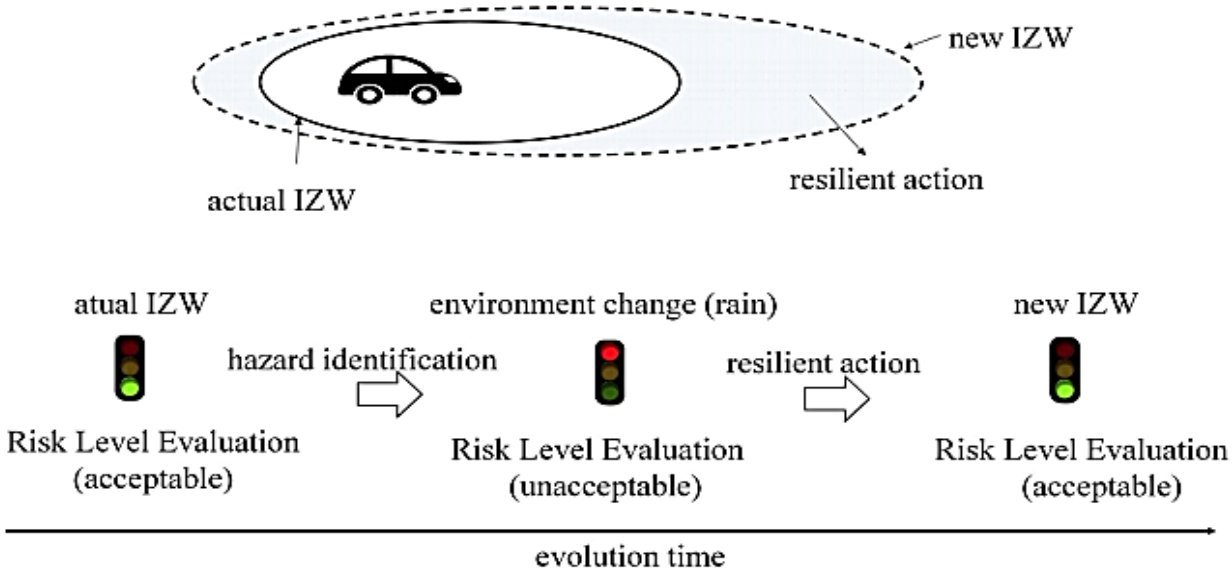

Figure 3 Risk Assessment of Autonomous Vehicles

The usage of electronic components and software modules is increasing in recent days as autonomous vehicles are in the pacing development. Like automated electric vehicles, automated electric and electronic system vehicles are designed. For such designs to be efficient, integration of the system, scalability, etc. is considered. CPS is widely employed for the electric and electronic automation of vehicles. This implementation is considered to be the most reusable module. Moreover, these designs are considered the simplest method for the integration of actuators, sensors, and controllers (Girdhar et al., 2022). CPS of autonomous vehicles is also designed to detect the flow of traffic in the environment. This is mainly done to enhance the planning in an offline mode before driving so that traffic-free roads are preferred so that poor connectivity during driving would not impose challenges. This method also aids in the speed selection, and brake timing respective to the distance. This method also has ad-hoc connectivity through which they are capable enough to connect with the nearby vehicles. The method is validated with the real-time data collected from the traffic environment through the sensors of CPS. The validation showed that offline traffic prediction helped in the efficiency of autonomous vehicles (Wang et al., 2023). The battery management of autonomous vehicles is another cause of concern. Hence proper battery management can improve the efficiency of the CPS (Yudhana et al., 2021). Autonomous vehicles find their application mostly in rescue and surveillance operations. For such operations, reliability and are safety much required as they are unmanned in remote areas. Autonomous vehicles are to be designed with ensured efficiency and safety of the system at the time of planning itself. (Majd, 2021). CPS that are reliable and secure is developed by considering case studies like SBW – Steer by Wire. For such consideration, CAN – Controller Area Networks are employed. This is mainly done to enhance the time and risk assessment of the CPS. The security constraints are mentioned in the earlier stages of the design scenario and are embedded. This provides the authentication, confidentiality, and data integrity of the system. The design mainly aims at the reliability of systems

through the employment of a controller area network. This method imposes ECU that helps in tolerating erroneous conditions (Koley et al., 2023)

Notion-based studies that include k-anonymity which is based on the client include real datasets and the performance of such anonymity is measured. The metrics presents for such design include utility and privacy metrics upon which the problems are analysed and optimum criterion is achieved. Grouping is done to achieve privacy of the contents in the group following which programming is done that calculated the grouping. The already grouped mechanisms and strategies are formulated together to obtain optimum anonymity. Through this, the optimum utility and privacy are achieved for the real data sets (Zheng et al., 2021). Safety enhanced measures are framed to ensure the safety of the road transport system. The structured framework is analysed with real simulation. The framework considers the real-time datasets and the efficiency of the system is seen in the results. It is a known fact that the road transport system is shared by both manual and autonomous vehicles hence the road transport system elements have been shared that help in handling the autonomous vehicle movement (Zheng et al., 2021) .The most common problem seen with the security and safety of autonomous vehicles is that they face crashes that fail to predict the real scenarios. As algorithms based on learning techniques are employed in autonomous vehicles, the characteristic feature of the operation time becomes unpredictable in the process of design. Moreover, verification of these learning algorithms is not possible in the process of design. For such unpredictable cases, a method known as the assurance of run time is incorporated. This assurance helps in the verification of the system correspondence to the addition of the small elements and finally, the verification of the output is done. If the verified output is safe, then it is allowed to pass and if the verified output is unsafe it is not allowed by the enforcer to pass through. This can be better understood with the example of a drone where the fly area of the drone is pre-specified. The enforcer monitors the drone activity and allows the drone to fly within the fenced area that is pre-specified and restricts the commands if the received command is out of eth pre-specified area and gives it a new command to fly. The latter is the unsafe output which is modified by the enforcer. With these verified and unverified scenarios, the system is safe by rejecting all the unsafe outputs received (Sivakumar et al., 2024).

The attacks imposed on autonomous vehicles are categorized into three systems namely autonomous control systems, autonomous components of driving systems, and communications that are a vehicle to everything. Protection against such attacks is further categorized as detection of an anomaly, architecture of security, and detection of intrusion. For such detections, machine learning techniques and artificial intelligence are employed. This review will aid in the enhanced research on attacks and security of autonomous vehicles (Kim et al., 2021).

3.2 Autonomous Vehicles path planning

Path planning is essential for self-driving cars, as it selects the safest and most effective routes by considering factors like traffic, road conditions, and the environment. There are two main types of path planning: global (offline) and local (online). Global path planning involves predefined routes based on detailed maps and static information, while local planning adjusts to real-time conditions as the vehicle is in motion. Offline planning refers to the process where routes are calculated in advance based on historical and expected traffic data. This method can significantly enhance performance by analysing traffic patterns, vehicles can avoid congested routes, leading to shorter travel times. It can incorporate safety measures by predicting potential hazards based on traffic data, thereby reducing accident risks.

Conversely, (Liu, 2021 #39) aimed to develop a robust lane-changing strategy for autonomous vehicles by considering both preceding and lagging vehicles, ensuring safety, comfort, and efficiency. It employed cubic polynomial interpolation for path and speed planning, alongside a comprehensive trajectory optimization function and a dynamic decoupling model for real-time applications. Simulations and real vehicle validations demonstrated that the method effectively generated satisfactory lane-changing trajectories, enhancing automatic lane-changing actions. In study (Akhshirsh, 2021 #40) focused on developing a cost-effective GPS-aided autonomous guided vehicle (AGV) using an Arduino Uno microcontroller and a mechanical radio-controlled rover for offline path planning. The algorithm implemented was based on shortest path calculations utilizing GPS data, with a magnetic digital compass for accurate heading. Results showed that the AGV could navigate to its destination with a positioning error within one meter, indicating its potential for applications such as landmine detection and removal.

The enhancement of performance and safety in autonomous vehicles through offline planning for traffic conditions involves a comprehensive approach that combines data analysis, advanced algorithms, simulation, and real-time integration. This multifaceted strategy not only improves operational efficiency but also significantly enhances the

safety of AVs on the road. However, challenges such as rapidly changing traffic conditions and sensor limitations in complex environments must be addressed to ensure the effectiveness of offline planning.

3.3 Different Defensive Techniques and their Trade-Offs

Defensive cyber security techniques in self-driving vehicles are crucial for ensuring safety and reliability in autonomous driving. The approaches such as firewalls, IDS, encryption protocols, security information and event management (SIEM) and endpoint protection platforms. These techniques aim to protect vehicles from various threats, including adversarial attacks and system failures. The table 2 illustrates comparison among various defensive techniques, focusing on their computational complexity, efficacy, and deployment feasibility.

The table 2 Illustrates Trade-offs among Different Defensive Methods

Defensive Techniques	Computational complexity	Efficacy	Deployment Feasibility
Firewall	Low to moderate	High	High
Instrusion Detection Systems (IDS)	Moderate to High	Moderate to High	Moderate
Encryption protocol	High	Very High	Moderate to High
SIEM	Very High	High	Low to moderate
EPP	Moderate	High	High

3.5 Real-time Solutions and Case Studies for Vehicle-To-Vehicle Communication

V2V communication is essential to faces the challenges in the AVs technologies that can be addressed by reliable methodology like ML and AI techniques. Those are crucial to deliver a secured and reliable AV technologies with CPS. The following practical case studies deliberates the challenges in V2V communication and how that has been tackled,

Case study 1 - Nissan's V2V Communication System

Nissan has integrated blockchain technology in its V2V communication systems to enhance security and ensure data integrity. This system helps in securely sharing critical information about road conditions and traffic.

Case study 2- Ford's Smart Mobility Initiative

Ford has implemented edge computing in its V2V systems to enhance reliability. By processing data locally, Ford reduces latency and improves response times for critical alerts.

Case study 3- Volkswagen's Traffic Management System

Likely, Volkswagen uses ML algorithms to analyze real-time traffic data collected from vehicles. This system predicts congestion patterns and optimizes traffic flow, demonstrating the effectiveness of ML in V2V applications.

4. Limitations in ML integrated with CPS for Autonomous Vehicle

From the review, it is perceived that the difficulty of the CPS as autonomous vehicles and the associated security concerns are addressed in maximum of the studies. It is clearly seen that there are only an insufficient studies are existing concerning the real-world situation among the vehicle transportations. It is also manifested that there are only inadequate studies obtainable on the supervisory with a human module on a real-world source. The challenges related with autonomous vehicles are not protected up in definite applications.

The challenges related with autonomous vehicles are high whereas the nature of the vehicle is inherent. Besides, the vehicle connection towards the external atmosphere is essential with the vital automatic adapting environment. As a

result of the simplicity, the vehicles can transfer data with the adjacent vehicles and its surroundings. The distinctive feature of autonomous vehicles can be in such a way that it do not depend on humanitarian support and the principles can be measured in the design method. Hence autonomous vehicles must be designed in such a way that they have capability of sufficient to deal with uncertainties however various challenges related with them make the devices with insufficient safety features.

Autonomous vehicles are exposed to the atmosphere where the parameters are also dynamic. The vehicles on one side receive information from the sensors by which the corresponding reliability actions are taken by the vehicle and on the other side, to the information received from the sensors the vehicle's automatic adaptation against the attacks also are initiated. Hence uncontrolled actions occur in the vehicle which is not the case in classic vehicles.

4.1 Safety Measures are not met in Autonomous Vehicles

ISO 26262 is an international functional safety standard that provides guidelines to minimize risks and ensure that automotive components function correctly in road vehicles. It aims to minimize risks associated with product design and development, thereby preventing hazards that could threaten human health and safety. As per the safety standard explicitly ISO26262 remains as a standard that is engaged in the safety of vehicles. The standard requires the tools, approaches, design, and methods to be utilized in the electronic and electrical design of a vehicle. While the requirements concerning with functional safety of the vehicle execute a high challenge toward the inventers as they have to be combined with the former design procedure. However the safety principles do not completely cover-up in the autonomous vehicles.

In addition, it employs a risk-based approach using Automotive Safety Integrity Levels (ASILs) to classify risks and ensure that safety measures are proportional to potential hazards. This structured framework is crucial for OEMs and suppliers to develop safe automotive systems throughout their lifecycle.

4.1.1. Data Privacy and Ethical Considerations in AVs

AVs system utilizes and produce an extensive data on how vehicles operate, passengers' actions, and the surrounding environment. It is crucial to safeguard the privacy of this data in order to uphold passenger trust and belief in AVs. Furthermore, ethical issues come up when it comes to AVs making decisions in crucial scenarios, like deciding between two possible collision results. Dealing with these worries involves creating strong regulations on data privacy and ethical principles for AV makers and operators.

4.1.2 Regulatory Compliance for AV

Various governments and regulatory bodies are creating extensive frameworks to oversee the development, testing, and deployment of autonomous vehicle (AV) technologies in order to address safety and security issues. These frameworks encompass regulations and standards related to cybersecurity, data privacy, safety certification, and ethical principles for AV usage. The goal of establishing precise regulatory guidelines is to guarantee the secure and accountable incorporation of AVs into public roads, while also promoting innovation and progress in the automotive sector.

Overall, the AV technologies and its concern on safety and security indicates a paradigm shift in transportation that leverages the road safety and reduces the accidents. Though, the AV technologies provides these benefits still there is a significant challenges like cyber-attacks, data privacy, adversarial attacks, and addressing ethical implications are prominent for obtain a maximum benefits from the AV technologies while safeguarding passenger care and security.

4.2 Environmental Ambiguity and Problems Related with ML

Autonomous vehicles are intended to operate in all conditions that are even under situations that are erratic and unmanageable. Hence autonomous vehicles fail under certain unpredicted conditions. Therefore the pre-designed safety measure becomes a failure at the time of the incident. Therefore the safety standards must be able to cover all the predicted scenarios so that the designers will consider them at the early stages of designing.

There are also issues and challenges in autonomous vehicles due to ML. Some of the issues with the usage of ML are they can change the encapsulation and boundary where the failure occurs as the maintenance of code becomes difficult. The unstable scenario also causes wrong calibrations due to the intervention of ML. These wrong calibrations cause a hidden correction in the signal.

To mitigate these challenges of CPS in AV can be addressed by implementing pre-trained Convolutional Neural Network (CNN) models for dynamic cyber-attack detection can enhance security within the CPS framework. Besides, utilizing simulation models allows researchers to test AV systems under various conditions without the costs associated with physical prototypes. This method can effectively assess performance and identify potential vulnerabilities before real-world deployment. Addition to that the adoption of 6G technology can significantly improve communication between V2V and infrastructure (V2I), enhancing data transmission speeds and reliability.

4.4 Unclear Validations

Autonomous vehicles are generally tested through validations. It does not mean that a vehicle that passed a test or two is more reliable as the testing scenario for AV is difficult for two main reasons, one is the repetitive test of certain algorithms will have the chance to miss certain cases and the other reason is multiple behaviours for such cases make it more complex. If such challenges are addressed then the future applications will find a better scope.

Moreover, the critical analysis is done based on the ML methods used in the CPS systems. Moreover, critical analysis is performed with regards to various parameters used by several prevailing methods for analysing the security in autonomous vehicles. The figure 4 depict the algorithms used in for security purpose and it is depicted below.

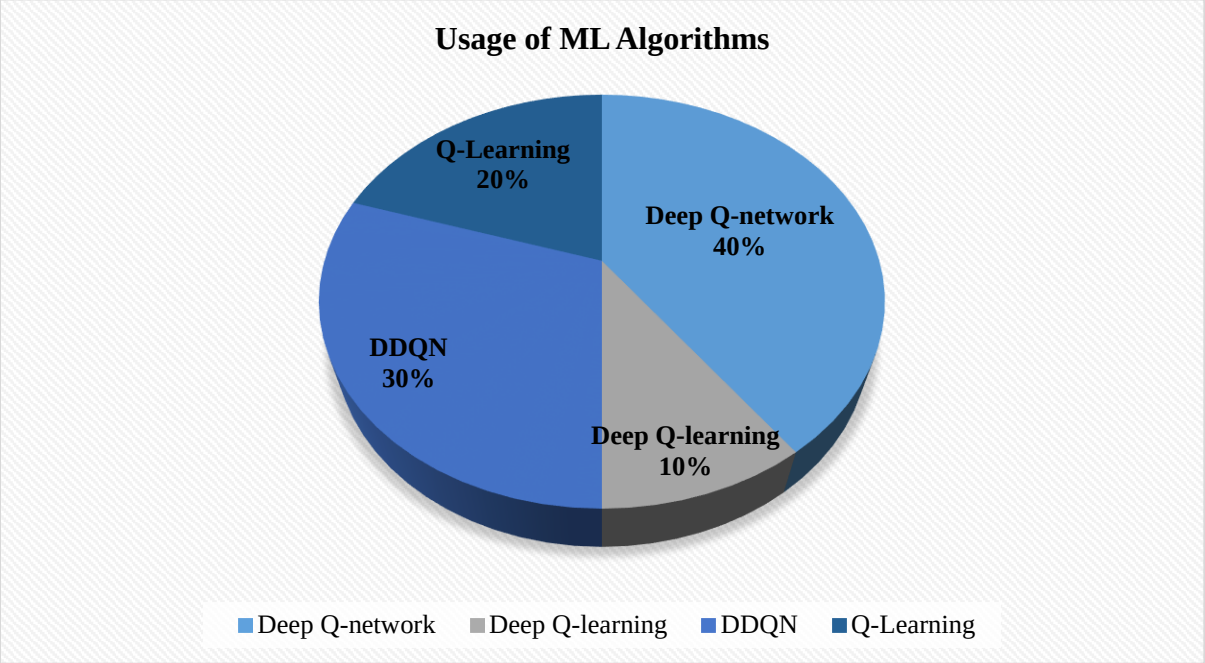

Figure 4 Critical Analysis for Usage of ML Algorithms

The figure 4 describes the usage of ML algorithms for the security concerns in CPS systems. From the figure it is inferred that the Deep Q-network is widely used compared with the Q-learning, DDQN and Deep-Q learning.

Findings:

- Integrating a "security by design" method with system classification to limit potential security measures.
- With lightweight encryption algorithms along with hardware-accelerated security operations to achieve real-world requirements lacking of cooperation in security system.
- Sensor systems in autonomous vehicles are exposed to security discord that can bring about safety problems.

5. Future Recommendation

In future the security of ML is incorporated with the CPS specifically in the framework of autonomous vehicles, comprises of various crucial areas of research and development. Besides, the incorporation of ML in CPS improves the functionality however it introduces a distinct security issues that can be addressed to confirm consistent safety. The areas has to be focused are given below:

- **Addressing security challenges**

When designing the autonomous systems has several security issues. There may be occurrence of complexity related with the intrinsic network for sensors and algorithms for autonomous vehicles. Hence, the system with security measures will be designed. For the issues related with the real-time problem can be deployed with lightweight encryption techniques with various hardware functions.

- **Challenges faced by ML**

  Availability of insufficient dataset can limit the effectiveness of ML-based detection systems. Moreover, conform that ML models are interpretable and consistent remains critical, specifically in autonomous vehicles implementation. It comprises the developing techniques to improve the ML decisions and its effects with safety systems.

- **Consistent Up gradation and Compliance**
  Because of the robust progression in field of cyber threats, automated vehicles should be prepared with mechanism for over-the-air (Wang et al.) updates to confirm that safety measures is effectual in evolution of vehicles. Besides, the adaptability is required to secure the different and evolving threats.

- **Monitoring Structures**

  The robust enhancement in autonomous vehicle technology regularly suppress prevailing regulations. Moreover, combined efforts between producers, experts in cyber-security and representatives are basis for the establishment and updation of regulations. Also it is needed by autonomous vehicles for a distinct security purpose.

6. Conclusion

The review paper mainly conducted to provide a thorough examination of the security measures relevant in CPS for AVs, specifically looking at how ML techniques are integrated within CPS to enhance cyber-attacks. The study also delved into the impact of CPS on AVs, the detection of vulnerabilities in CPS using ML algorithms, and the benefits of CPS as a reusable module in terms of cost savings and development time. The paper further investigated the key aspect of risk assessment related to autonomous vehicles, highlighting that performance can be significantly enhanced when risk assessments are validated by large datasets during the training phase, especially when using learning models. It also discussed real-world applications of V2V communication, with a focus on improving passenger safety and security. Moreover, the study elaborated the ethical consideration need to be consider while designing the AVs and the future trends in the autonomous driving system. In conclusion, the findings underscore the importance of utilizing advanced data analytics and ML techniques to enhance the security and dependability of CPS for self-driving cars, ensuring safe operations in increasingly complex traffic environments.

REFERENCES

Adepu, S., Kandasamy, N. K., Zhou, J., & Mathur, A. (2020). Attacks on smart grid: Power supply interruption and malicious power generation. *International Journal of Information Security*, *19*, 189-211.

Agrawal, N., & Kumar, R. (2022). Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. *ISA transactions*, *130*, 10-24.

Aldhyani, T. H., & Alkahtani, H. (2022). Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. *Sensors*, *22*(1), 360.

AlEisa, H. N., Alrowais, F., Allafi, R., Almalki, N. S., Faqih, R., Marzouk, R., Alnfiai, M. M., Motwakel, A., & Ibrahim, S. S. (2023). Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning. *IEEE Transactions on Consumer Electronics*, *70*(1), 1736-1746.

Alsulami, A. A., Al-Haija, Q. A., Alturki, B., Alqahtani, A., & Alsini, R. (2023). Security strategy for autonomous vehicle cyber-physical systems using transfer learning. *Journal of Cloud Computing*, *12*(1), 181.

Anumba, C. J., & Roofigari-Esfahan, N. (2020). *Cyber-Physical Systems in the Built Environment*. Springer.

Arrieta, A., Valle, P., & Ali, S. (2024). Search-based Automated Program Repair of CPS Controllers Modeled in Simulink-Stateflow. *arXiv preprint arXiv:2404.04688*.

Aziz, W. A., Ioannou, I., Lestas, M., Qureshi, H. K., Iqbal, A., & Vassiliou, V. (2023). Content-aware network traffic prediction framework for quality of service-aware dynamic network resource management. *IEEE Access*.

Bashendy, M. S., Tantawy, A., & Erradi, A. Autonomous Response Agent for Cyber Physical System Attacks: A Model-Free Deep Reinforcement Learning Approach (Drl-Irs). *Available at SSRN 4716080*.

Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, *24*(4), 3614-3637.

Bharathi, V. (2024). Vulnerability detection in cyber-physical system using machine learning. *Scalable Computing: Practice and Experience*, *25*(1), 577-591.

Catillo, M., Pecchia, A., & Villano, U. (2023). CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders. *Computers & security*, *129*, 103210.

Conrad, C., Al-Rubaye, S., & Tsourdos, A. (2023). Intelligent embedded systems platform for vehicular cyber-physical systems. *Electronics*, *12*(13), 2908.

Dhiman, A., Gupta, K., & Sharma, D. K. (2021). Machine learning for fostering security in cyber-physical systems. *Security in Cyber-Physical Systems: Foundations and Applications*, 91-122.

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*, 1674-1683.

Fei, X., Shah, N., Verba, N., Chao, K.-M., Sanchez-Anguix, V., Lewandowski, J., James, A., & Usman, Z. (2019). CPS data streams analytics based on machine learning for Cloud and Fog Computing: A survey. *Future generation computer systems*, *90*, 435-450.

Feng, Y., Hu, B., Hao, H., Gao, Y., Li, Z., & Tan, J. (2018). Design of distributed cyber–physical systems for connected and automated vehicles with implementing methodologies. *IEEE Transactions on Industrial Informatics*, *14*(9), 4200-4211.

Girdhar, M., You, Y., Song, T.-J., Ghosh, S., & Hong, J. (2022). Post-accident cyberattack event analysis for connected and automated vehicles. *IEEE Access*, *10*, 83176-83194.

Gougeon, P., & Hamelin, E. (2023). Development complexity of Cyber-Physical Systems: theoretical and practical benefits from Pre-Integrated Architectures. *Journal of Smart Environments and Green Computing*, *3*(1), 3-17.

Guo, J., Li, L., Wang, J., & Li, K. (2022). Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks. *IEEE Transactions on Industrial Informatics*, *19*(5), 6624-6635.

Harrison, K., Ingole, R., & Surabhi, S. N. R. D. (2024). Enhancing Autonomous Driving: Evaluations Of AI And ML Algorithms. *Educational Administration: Theory and Practice*, *30*(6), 4117-4126.

Hoepfner, G., Nachmann, I., Zerwas, T., Berroth, J. K., Kohl, J., Guist, C., Rumpe, B., & Jacobs, G. (2023). Towards a holistic and functional model-based design method for mechatronic cyber-physical systems. *Journal of Computing and Information Science in Engineering*, *23*(5), 051001.

Jamal, A. A., Majid, A.-A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. *Materials Today: Proceedings*.

Khanfar, N. O., Ashqar, H. I., Elhenawy, M., Hussain, Q., Hasasneh, A., & Alhajyaseen, W. K. (2022). Application of unsupervised machine learning classification for the analysis of driver behavior in work zones in the state of Qatar. *Sustainability*, *14*(22), 15184.

Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, 102150.

Koley, I., Dey, S., Mukhopadhyay, D., Singh, S., Lokesh, L., & Ghotgalkar, S. V. (2023). CAD Support for Security and Robustness Analysis of Safety-critical Automotive Software. *ACM Transactions on Cyber-Physical Systems*, *7*(1), 1-26.

Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine learning for security and the internet of things: the good, the bad, and the ugly. *IEEE Access*, *7*, 158126-158147.

Lv, C., Hu, X., Sangiovanni-Vincentelli, A., Li, Y., Martinez, C. M., & Cao, D. (2018). Driving-style-based codesign optimization of an automated electric vehicle: A cyber-physical system approach. *IEEE Transactions on Industrial Electronics*, *66*(4), 2965-2975.

Lv, Z., Chen, D., Lou, R., & Alazab, A. (2021). Artificial intelligence for securing industrial-based cyber–physical systems. *Future generation computer systems*, *117*, 291-298.

Majd, A. (2021). DIANA: Distributed and Safe Autonomous Navigation for a Swarm of Autonomous Vehicles.

Meng, T., Hu, M., Bian, Y., Chew, C.-M., Song, Z., Yang, D., Zhong, Z., & Huang, J. (2023). Integrated Design Framework for Perception System of Automated Electric Vehicles with Enhanced Sensor Reusability. *IEEE Transactions on Transportation Electrification*.

Mishra, A., Jha, A. V., Appasani, B., Ray, A. K., Gupta, D. K., & Ghazali, A. N. (2023). Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective. *International Journal of System Assurance Engineering and Management*, *14*(Suppl 3), 699-721.

Nagar, D., Raghav, S., Bhardwaj, A., Kumar, R., Singh, P. L., & Sindhwani, R. (2021). Machine learning: best way to sustain the supply chain in the era of industry 4.0. *Materials Today: Proceedings*.

Nalic, D., Pandurevic, A., Eichberger, A., & Rogic, B. (2020). Design and implementation of a co-simulation framework for testing of automated driving systems. *Sustainability*, *12*(24), 10476.

Neema, H., Nine, H., & Roth, T. (2023). Reusable Network Simulation for CPS Co-Simulations. In *Proceedings of Cyber-Physical Systems and Internet of Things Week 2023* (pp. 122-129).

Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. *IEEE Communications Surveys & Tutorials*, *23*(1), 524-552.

Pavithra, R., Kaliappan, V. k., & Rajendar, S. (2023). Security Algorithm for Intelligent Transport System in Cyber-Physical Systems Perceptive: Attacks, Vulnerabilities, and Countermeasures. *SN Computer Science*, *4*(5), 544.

Pereira, A., & Thomas, C. (2020). Challenges of machine learning applied to safety-critical cyber-physical systems. *Machine Learning and Knowledge Extraction*, *2*(4), 579-602.

Pundir, A., Singh, S., Kumar, M., Bafila, A., & Saxena, G. J. (2022). Cyber-physical systems enabled transport networks in smart cities: Challenges and enabling technologies of the new mobility era. *IEEE Access*, *10*, 16350-16364.

Ruan, H., Dorneanu, B., Arellano-Garcia, H., Xiao, P., & Zhang, L. (2022). Deep learning-based fault prediction in wireless sensor network embedded cyber-physical systems for industrial processes. *IEEE Access*, *10*, 10867-10879.

Saghezchi, F. B., Mantas, G., Violas, M. A., de Oliveira Duarte, A. M., & Rodriguez, J. (2022). Machine learning for DDoS attack detection in industry 4.0 CPPSs. *Electronics*, *11*(4), 602.

Salahdine, F., & Kaabouch, N. (2020). Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. *Physical Communication*, *39*, 101001.

Sheikh, Z. A., Singh, Y., Singh, P. K., & Ghafoor, K. Z. (2022). Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope. *Computer Communications*, *193*, 302-331.

Sivakumar, M., Belle, A. B., Shahandashti, K. K., Odu, O., Hemmati, H., Kpodjedo, S., Wang, S., & Adesina, O. O. (2024). I came, I saw, I certified: some perspectives on the safety assurance of cyber-physical systems. *arXiv preprint arXiv:2401.16633*.

Sun, H.-T., Peng, C., Ge, X., & Chen, Z. (2023). Secure event-triggered sliding control for path following of autonomous vehicles under sensor and actuator attacks. *IEEE Transactions on Intelligent Vehicles*, *9*(1), 981-992.

Wang, X., Ahmad, I., Javeed, D., Zaidi, S. A., Alotaibi, F. M., Ghoneim, M. E., Daradkeh, Y. I., Asghar, J., & Eldin, E. T. (2022). Intelligent hybrid deep learning model for breast cancer detection. *Electronics*, *11*(17), 2767.

Wang, Z., Keo, P., & Saberi, M. (2023). Real-time traffic state measurement using autonomous vehicles open data. *IEEE Open Journal of Intelligent Transportation Systems*.

Xi, L., Wang, R., & Haas, Z. J. (2022). Data-correlation-aware unsupervised deep-learning model for anomaly detection in cyber–physical systems. *IEEE Internet of Things Journal*, *9*(22), 22410-22421.

Yudhana, A., Mukhopadhyay, S., Prima, O. D. A., Akbar, S. A., Nuraisyah, F., Mufandi, I., Fauzi, K. H., & Nasyah, N. A. (2021). Multi sensor application-based for measuring the quality of human urine on first-void urine. *Sensing and Bio-Sensing Research*, *34*, 100461.

Zheng, W., Guo, Q., Yang, H., Wang, P., & Wang, Z. (2021). Delayed propagation transformer: A universal computation engine towards practical control in cyber-physical systems. *Advances in Neural Information Processing Systems*, *34*, 12141-12153.

Zhu, Q., Sangiovanni-Vincentelli, A., Hu, S., & Li, X. (2018). Design Automation for Cyber-Physical Systems [Scanning the Issue]. *Proceedings of the IEEE*, *106*(9), 1479-1483.