[1]Venkata Lakshmi Namburi

Enhancing Autonomous Vehicle Security through Software-Defined Networking and Ai-Driven Threat Detection

Journal of Electrical Systems

Abstract: - The increasing digital footprint of autonomous vehicles, in conjunction with the advent of technologies connected to artificial intelligence, has increased the potential for cyber vulnerabilities. This is a result of both factors. The three levels that comprise an autonomous driving system are the Sensor Layer, the Communication Layer, and the Control Layer. When seen from an attacker's perspective, these levels include the most crucial components. Regarding the sensor layer, some sensors constantly monitor the dynamics of the environment and the vehicle around it. On the other hand, these sensors are vulnerable to eavesdropping, jamming, and spoofing attacks. The communication layer combines both near-field and far-field communications to permit communication between more edge sensors in the area and faraway edge data centres. This connectivity is necessary to facilitate communication. The 'man-in-the-middle' assault and the Sybil attack can exploit this layer. Functionalities of an autonomous driving system, such as the automation of a vehicle's speed, braking, and steering, are made possible by the control layer, which is located at the very top of the hierarchy. Implementing artificial intelligence into software-defined vehicles paves the way for a wide range of options that could transform the landscape of automotive technology and mobility. Additionally, these prospects have the potential to revolutionize the industry.

Keywords: Autonomous vehicle, Software-defined vehicle, AI.

Introduction

The development and operation of autonomous cars are currently aided by artificial intelligence (AI). Autonomous vehicles are safer and more efficient than human drivers because they employ artificial intelligence algorithms to navigate, observe, and adapt to fluid situations. Future autonomous vehicles are expected to include even more advanced capabilities and safety features as artificial intelligence (AI) technology improves. There has been a revolutionary shift in the evolution of autonomous systems due to the application of artificial intelligence (AI). This groundbreaking combination can revolutionize conventional development procedures, boosting productivity and speeding the pace of innovation. There is a paradigm shift toward Software-Defined cars (SDVs) due to the incorporation of artificial intelligence technology into several aspects of software development for autonomous vehicles [1-4].

Benefits of AI Algorithms for Autonomous Vehicles

In autonomous vehicles, artificial intelligence algorithms are currently impacting various stages, ranging from the initial coding to post-deployment maintenance [3]. The following are some of the advantages that can be gained:

Safety: Eliminating human error can greatly reduce the number of accidents, which will ultimately lead to safer roads.

Traffic Flow: To alleviate congestion and improve efficiency, platooning [4] and efficient routing can be utilized.

Accessibility: People of any age, including those with disabilities, the young, and the old, can walk independently.

Energy Savings: The consumption of gasoline and pollution are both reduced when driving is optimized.

Productivity and Convenience: Passengers can make better use of their travel time, while delivery services can improve their efficiency.

The application of artificial intelligence in autonomous vehicles is positioned for a prosperous future. This will create fascinating opportunities and shape everyday life. Figure 1 presents a glimpse of the available opportunities.

[1] Research Scholar, B.E.S.T Innovation University (BESTIU), Software Systems Engineer, Danlaw Inc. Michigan USA. venkatanamburi91@gmail.com

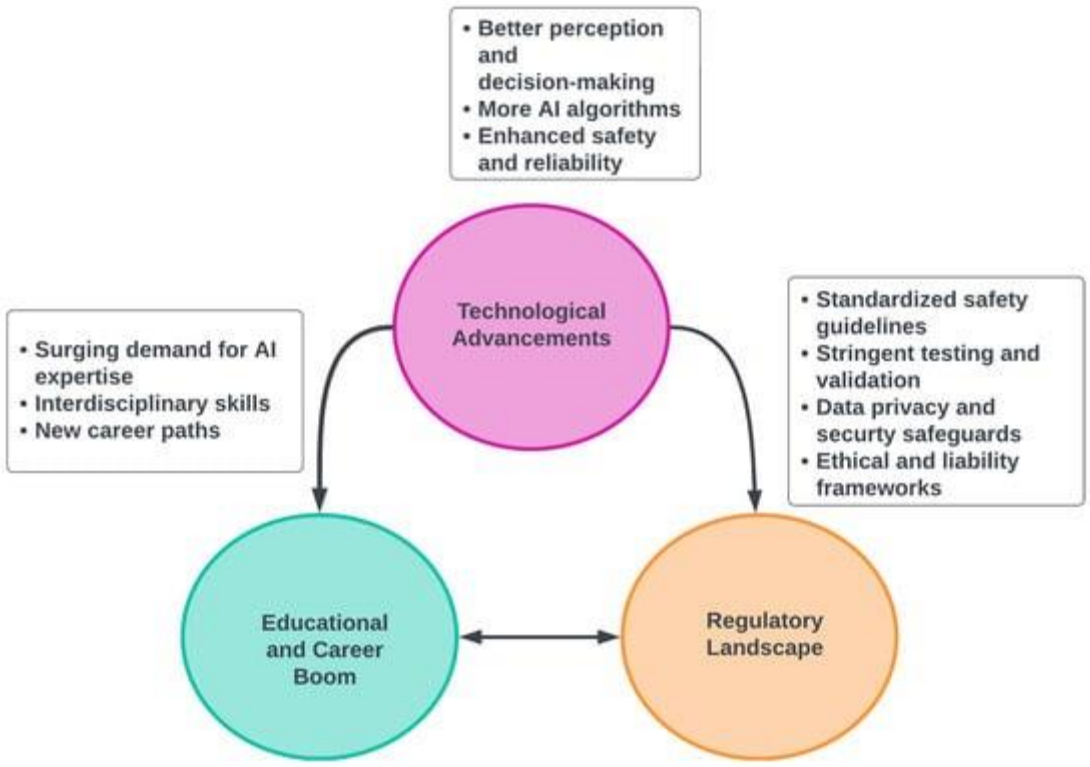

Figure 1. Benefits of AI in autonomous vehicles.

Cybersecurity vulnerabilities have been reported by hackers who wear grey or white hats. According to these hackers, vehicles with advanced driver assistance systems are vulnerable to cyberattacks. One example is the 2022 demonstration of two assaults by Chinese researchers from Keen Security Labs using a Tesla Model S's integrated camera system. Deep learning models used by autonomous vehicles (AVs) to mimic human cognitive abilities are only partially safe, according to researchers from other institutions. Unmodeled hazards and unexpected obstacles to safety, in addition to the fact that these models are highly attackable, could compromise the regular functioning of AVs [3].

Security professionals are shifting their attention toward proactive protection methods to address the growing threat of cyberattack vehicles. One of the most critical aspects of this strategy is the idea of "security by design." This concept stresses the need to build security features into technical systems from the ground up rather than adding them on later or as a retrofit. Incorporating security considerations into the design of the technology from the outset is guaranteed by this proactive posture [4]. Encrypting data transfers, authenticating communication participants, regularly upgrading software and firmware, and utilizing intrusion detection prevention systems (IDPS) are the most significant security measures that can be implemented within the security context by design [5].

Literature review

An operational design domain (ODD) is a set of detailed guidelines for how an autonomous vehicle (AV) should behave to ensure pedestrian safety. As can be seen in Figure 2, these examples exhibit the unique development of operational design domains (ODDs) [7] across a wide range of vehicle types, including automobiles and trucks, as well as in a variety of geographical areas, including the United States of America, China, and Europe. Instead of covering every company or region, this page will only summarize the many ODDs prevalent in many industries. Table 1 gives a complete mapping of different vehicle businesses, countries, and ODDs, as well as the driving situations that each firm is now addressing. It also explains the current landscape of the autonomous vehicle sector.

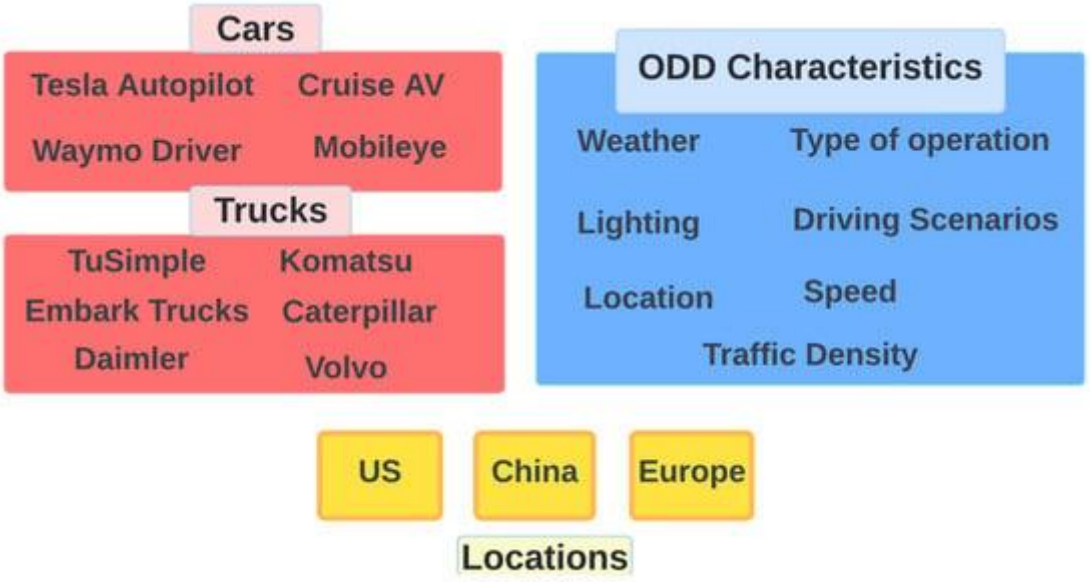

Figure 2. The current state of the industry: various vehicles from various places and their Operational Design Domain (ODD) features.

Waymo Driver: [9] Despite speed limitations and geo-fencing restrictions, it is possible to drive in a broader range of weather conditions on city streets and highways.

Tesla Autopilot: [10] This is most commonly used for travelling in a supervised environment on motorways with clearly delineated lanes at specific speeds.

Mobileye Cruise AV: [11] can only function on dry, sunny roads with marked lanes and speeds less than 45 mph.

Aurora and Waymo Via: A complete range of weather conditions, including daytime snow and light rain. Situations such as sunrise and sunset lighting, decently paved country roads and multi-lane highways, day and night operation, moderate traffic density, dynamic route planning, traffic light and stop sign recognition, intersection navigation, yard and warehouse manoeuvring, and similar scenarios are all within the realm of possibility.

TuSimple and Embark Trucks: [12] Excellent visibility, bright sunshine, and no precipitation. This vehicle needs to be able to withstand temperatures between -10 degrees Celsius and 40 degrees Celsius, drive only during the day, have clearly marked lanes, reach a maximum speed of 70 miles per hour, navigate through minimal traffic, follow pre-mapped routes, change lanes, merge and exit highways, platoon with other autonomous vehicles, and so on.

Pony.ai and Einride: Snow and torrential rain are among the weather conditions. There are many things to consider, such as the complex urban environment with its varied lighting conditions, residential areas, parking lots, and small city streets. Among these characteristics include low speeds (often between 20 and 30 mph), heavy traffic, numerous stops and turns, delivery zones that are geofenced, the ability to detect and avoid bikes and pedestrians, the ability to avoid obstacles in tight places, and the ability to reroute due to traffic dynamically.

Komatsu Autonomous Haul Trucks, Caterpillar MineStar Command for Haul Trucks: Harsh weather conditions include dust, heat, and very high temperatures. Problems with network connectivity, unleveled terrain, steep inclines and dips, pre-programmed routes, high ground clearance, obstacle detection in unstructured environments, path planning around natural hazards, dust and fog mitigation, and similar issues are all possible.

Baidu Apollo: Some places, such as Beijing and Shenzhen, have expressways and city streets. It can run day and night under ideal circumstances of clear weather and minimal traffic density. It was built with the express purpose of serving the robotaxis and passenger transportation industries. Specific scenarios include navigating through intersections, changing lanes, merging and exiting highways, recognizing stop signs and traffic lights, and navigating low-speed urban environments.

WeRide: Both Guangzhou and Nanjing utilize urban streets and roadways with limited access. With clear skies, operations can take place at any time of day or night. Last-mile delivery and robotaxi services are intended to be targeted. In particular, this technology has the potential to enable lane changes, highway merging and exiting, identification of traffic signals and stop signs, routing through intersections, and automated passenger and delivery pickup and drop-off.

Bosch and Daimler [13]: Motorways and other forms of roadways are present throughout Germany. Given suitable weather conditions, it might carry out its duties at any time of day or night. The only purpose is to facilitate applications related to highway transport. Potential particularities include communication with traffic control systems, automatic lane changes and overtaking, platooning with other AV trucks, and emergency intervention protocols.

H. J. Vishnukumar and colleagues [14] observed that conventional development approaches, such as Waterfall and Agile, must be revised when testing complex autonomous vehicles. They incorporated in-lab and field-based testing and validation into their groundbreaking AI-powered ADAS and autonomous system testing and validation (T&V) technique. The AI system's brain can learn from past test scenarios, create new efficient cases, and control different simulated conditions via machine learning and deep neural networks, allowing for comprehensive testing.

When critical testing is completed, they are followed by validation in the real world using automated cars in controlled environments. Saving time during development and enhancing the efficacy and quality of autonomous systems are both made possible by continuously learning from each testing iteration and applying that knowledge to future testing. A safer and more dependable future for autonomous vehicles is possible thanks to the suggested technique, which eventually lays the groundwork for AI to handle most to-and-from duties.

The algorithms necessary for performing a range of tasks in autonomous driving were described by Bachute, Mrinal R., and colleagues [15], considering the system's complexity. Using the "Locally Decorrelated Channel Features (LDCF)" method for improved pedestrian recognition and Reinforcement Learning (RL) models for effective velocity management in car-following situations are just two examples of the system's ability to recognize specific algorithmic preferences for tasks. In motion planning, imbalanced data defect diagnostics, vehicle platoon scenarios, and other fields, the research emphasizes the importance of algorithmic decisions. To address the dynamic challenges linked to autonomous driving, it advocates for the continuous improvement and extension of algorithms. This lays a solid groundwork for further research into how the autonomous driving system works, what kinds of tasks it can handle, and what algorithms it can learn and apply. In particular, this is a groundwork that will facilitate additional research.

According to Y. Ma and colleagues [16], AI is a key factor propelling AVs' research, development, and introduction into the transportation sector. While previous studies have examined various facets of AI's potential in AV development, AI is now crucial for AVs to perceive their environment and make educated decisions while driving. AI relies on massive amounts of data from numerous sensors and powerful computational capabilities. This paper aims to fill a gap in the current literature by critically evaluating critical works on the topic.

The primary topic of this study is the analysis of how artificial intelligence is used to support essential applications in autonomous vehicles (AVs). These applications include perception, localization and mapping, and decision-making. This study examines existing methods to shed light on the application of artificial intelligence, shedding light on the accompanying difficulties and problems. In addition, it examines how AI may be better integrated with new technologies to enhance simulation platforms. These include 5G connectivity for connected autonomous vehicles, HD maps, big data, HPC, AR, and VR. This examination also highlights opportunities that may arise.

To put it simply, this study is an excellent reference for researchers who are interested in gaining a more in-depth understanding of artificial intelligence's function in autonomous vehicle research. It provides an exhaustive analysis of current procedures and opens the door for potential new advancements. According to research by G. Bendiab et al. [17], autonomous vehicles (AVs) have many advantages, such as less pollution and more safety. However, there are serious worries about security and privacy flaws.

Integrating blockchain technology and artificial intelligence presents a promising way to solve these concerns. Using both technologies' strengths, AV systems can be strengthened to withstand hostile attacks. The study

emphasizes the need for additional research to fully understand the potential of this combination in safeguarding autonomous vehicles (AVs). This is done through a thorough examination of security threats, current literature, and future research objectives. While several studies have looked at this junction, further work is needed to make the most of this opportunity.

M. Chu et al. [18] state that autonomous vehicles (AVs) have given rise to a new occupation category called "safety drivers." These motorists are responsible for directing and controlling AVs while carrying out various driving duties. Although safety drivers' perspectives are crucial to road testing, they are underappreciated in the Human-Computer Interaction (HCI) community. Interviews with 26 safety drivers revealed that while working with AVs, they had to cope with inaccurate algorithms, change their perspective, and overcome obstacles like taking on risks associated with the AV industry's upstream and having few chances for professional development. Additional research on human-AI interaction and the real-life experiences of safety drivers is needed in light of this finding.

M. H. Hwang and colleagues [19] created the Comfort Regenerative Braking System (CRBS) using neural networks to enhance the comfort drivers of driverless vehicles

feel.

The CRBS's ability to estimate acceleration and deceleration limitations based on passenger comfort parameters allows it to change vehicle management techniques, thereby reducing pain experienced during braking. Numerical analysis and backpropagation techniques make regenerative braking effective while remaining within acceptable parameters. A possible solution for autonomous electric vehicles, the simulated and proposed CRBS enabled efficient regenerative braking without sacrificing passenger comfort.

Critical advancements in IDPs for autonomous driving include:

- Machine Learning and AI Integration: Businesses are implementing AI and machine learning techniques to enhance the efficacy and precision of intrusion detection. These systems are more resilient to ever-evolving threats because they can learn from past data and adjust to new attack vectors.

- Anomaly Detection Techniques: AV IDPS used sophisticated anomaly detection techniques to find deviations from predicted behaviour. By utilizing these strategies, the system can identify unique attacks that may not correspond to previously identified attack patterns.

- Real-time Threat Analysis: To detect and react to potential dangers as they emerge, autonomous vehicles' IDPS work in real-time, processing data streams as they arrive from several sensors and vehicle components.

- Collaborative Threat Intelligence: Some methods involve merging shared databases of threat intelligence; this allows cars to share information, learn from each other, and react collectively to new threats as they arise.

This table gives a synopsis of a few companies, their products, and their market uses. The report also details the types of people employing these cybersecurity solutions for autonomous vehicles.

Table 1: synopsis of a few companies

Company	**Products/Research**	**Users**	**Usage**
Argus Cyber Security	Argus Connectivity Protection, Argus Lifespan Protection	Automotive OEMs, Tier 1 suppliers	In a variety of vehicle architectures, including electronic control units (ECUs), telematics, and information and entertainment systems
Symantec (now part of Broadcom)	Symantec Integrated Cyber Defense Platform	Automotive manufacturers, suppliers	To provide comprehensive threat management and protection in automotive systems
Harman	Harman's ECUSHIELD, TCUSHIELD	Automotive OEMs, telematics units	Protecting against cyberattacks for telematics and in-vehicle data systems

Cisco	Cisco's automotive cybersecurity solutions	Connected vehicle manufacturers, infrastructure providers	The incorporation of cybersecurity solutions into infrastructure and networks for connected vehicles

Securing AVs with Blockchain

In connected Autonomous Vehicle (AV) services, blockchain technology provides several options to improve security. Its one-of-a-kind qualities make it a potentially helpful answer for a number of the most critical problems that are associated with this field, including the following:

Data Integrity and Traceability: The immutability intrinsic to blockchain technology means that once data is recorded, it cannot be changed without being discovered. Logs of travel, readings from sensors, and records of maintenance are all examples of this type of data. Such traceability is necessary for diagnosing problems, resolving disputes regarding liability in the event of accidents, and preventing tampering.

Secure Communication: Blockchain technology can make vehicle-to-infrastructure (V2X) communication more secure and reliable. Due to blockchain's distributed ledger technology, automated cars can verify and trust messages from other vehicles or infrastructure without relying on a central authority. Specifically, this helps combat spoofing attacks, in which malicious actors provide fake information to antivirus appliances.

Decentralized Operations: Blockchain technology is based on a decentralized network, in contrast to the old types of centralized networks. The system is more resistant to cyberattacks because of its decentralized nature, which eliminates the possibility of a single catastrophic point. In the case of AVs, this might mean a less susceptible network for vehicle coordination and communication that is more robust overall.

Identity Management and Authentication: It is possible to employ blockchain technology to handle digital identities in an AV ecosystem in a secure manner. Only approved devices, cars, and infrastructure can communicate with one another, which is made possible through the utilization of cryptographic keys for identity verification. Vehicle systems can be protected against unwanted access and control due to this measure.

Smart Contracts for Automated Transactions: AVs can leverage intelligent contracts based on blockchain technology to conduct automated, secure, and transparent transactions. This is vital for services like automated parking fees, toll payments, and even peer-to-peer energy exchanges in the context of electric driverless vehicles.

Supply Chain Transparency: Additionally, blockchain can improve the safety of the AV supply chain. By monitoring the manufacturing, shipping, and installation of car components, blockchain technology can guarantee the genuineness of the components and prevent the use of counterfeit components, which could threaten the system's safety.

Data Sharing and Privacy: Blockchain technology permits careful and selective data sharing. Autonomous vehicles (AVs) produce a significant quantity of data, and blockchain technology can ease the sharing of this data with other parties (such as traffic control systems or other vehicles) to protect users' privacy and the security of their data.

The domain of intelligent vehicle (IV) communication has been significantly advanced by many research publications since 2020, all of which have used blockchain technology uniquely. The development of reliable and secure intravenous communication systems has been the focus of some research. Many different avenues of inquiry into accident aftermath and human safety have also been investigated. An example would be a crypto IV-TP-based reward system emphasizing precise accident data. In addition, cutting-edge Multi-Agent AIM (MAAIM) systems are visible; these systems use V2I/I2V communication enhanced by blockchain technology to handle the safe passage of vehicles through junctions expertly.

Another study area is the real-time interchange of connected and autonomous vehicle data. This effort is more important than ever, with new cyber dangers cropping up. A significant obstacle for AV systems might be cyberattacks, particularly Denial-of-Service (DoS) attacks. One attack that could compromise the system's functionality is sending a flood of fake requests. The general safety of Internet of Things devices is enhanced, while AV service performance and scalability are both improved.

Finally, Plug-in Hybrid Electric Vehicles (PHEVs) that function within smart grids have also been created with localized Peer-to-Peer (P2P) power trading models. The goal of this model is to maximize expenses while simultaneously improving trustworthiness and social welfare. To provide transaction security, privacy protection, user pleasure, and cost reduction or attainment of the best prices, localized P2P electricity trading systems can adopt an iterative double auction method. This allows auctioneers to bid prices. This extensive body of research highlights the wide range of possibilities and threats in the rapidly developing area of intravenous communication using blockchain technology.

The opportunities AI brings to SDVs

Enhanced Autonomous Driving

The primary benefit of AI to SDVs is the improvement of autonomous driving skills. Artificial intelligence (AI) allows cars to correctly understand their environments via tools like computer vision and natural language processing (NLP). Systems like this provide fast, accurate, and reliable object detection, traffic sign recognition, and decision-making similar to human judgment. According to industry analysts, autonomous vehicles are expected to account for as much as 15% of all vehicle sales by 2030, indicating a thriving global market for these vehicles.

Improved Vehicle Performance

AI is also an essential component in improving vehicle performance. Artificial intelligence algorithms can alter engine characteristics for the best fuel efficiency and performance, tweak suspension settings for greater comfort, and more effectively control energy use in electric vehicles. This is accomplished by analyzing data from a variety of sensors in real-time. Not only does this make driving more enjoyable, but it also helps to reduce emissions and energy consumption, which in turn contributes to a more sustainable environment.

Personalized Driver Experience

Another area that is strongly impacted by artificial intelligence is personalization. Self-driving vehicles (SDVs) powered by artificial intelligence can learn from the actions and preferences of their users to provide a more personalized driving experience. AI makes every ride more personalized for the driver and passengers by doing things like adjusting the temperature inside the vehicle and choosing music based on the driver's mood or the time of day. Further, voice assistants endowed with artificial intelligence can offer an interactive and responsive user interface, thereby improving the convenience and safety of vehicle operations.

Predictive Maintenance

The power of artificial intelligence to revolutionize car maintenance is demonstrated via predictive maintenance. Artificial intelligence can anticipate probable problems before they occur by assessing data from the operational history of the vehicle in conjunction with real-time inputs from various sensors. Treating problems in a proactive rather than reactive manner ensures increased reliability and safety and dramatically reduces the costs at which maintenance is performed.

Advanced Cybersecurity Measures

The significance of cybersecurity is growing as the number of connected automobiles increases. To protect essential vehicle systems and sensitive user data from being accessed or manipulated by unauthorized parties, artificial intelligence provides powerful solutions that can detect and mitigate potential cyber threats in real-time. Because of its capacity to adjust to ever-changing dangers, artificial intelligence is a vital weapon in the armoury of cybersecurity tools for small and medium-sized enterprises (SDVs).

Generative AI for Synthetic Data Creation

Extensive datasets are required to train artificial intelligence models for autonomous driving. These datasets might be challenging to compile, particularly for driving conditions that are uncommon or dangerous. Creating realistic synthetic data is one of the solutions offered by generative artificial intelligence. This allows for the simulation of a variety of settings without the dangers and expenditures that are connected with the collection of data from the actual world. During the training process, this exposes autonomous driving systems to a more extensive variety of scenarios, speeding up the development of these systems and improving their reliability and safety.

The challenges of integrating AI with SDVs

Integrating artificial intelligence with software-defined vehicles opens up a wide range of opportunities that could dramatically improve the functionality and efficiency of these vehicles. On the other hand, this integration presents some difficulties. All stakeholders involved in developing and deploying SDVs need to work together to overcome these limits, which are not only technical but also ethical, legal, and infrastructure-related.

Data Security and Privacy

Assuring the safety and confidentiality of the enormous amounts of data gathered and processed by AI in SDVs is one of the most significant difficulties. The fact that these cars rely on continuous data interchange to navigate, learn, and make judgments raises substantial issues regarding the privacy of its users and the possibility of data breaches. The automotive industry is becoming increasingly the target of cyberattacks. Only in the year 2023, 295 cybersecurity incidents occurred in the automotive and mobility arena. Of these attacks, 64 per cent were carried out by bad actors to cause harm. It is a complex undertaking that demands powerful cybersecurity measures and constant monitoring to keep this data from being accessed by unauthorized parties while guaranteeing compliance with global data protection requirements such as the General Data Protection Regulation (GDPR) in Europe.

Regulatory Landscape

Artificial intelligence (AI) in software-defined vehicles (SDVs) is still developing, and policymakers must assist to keep up with the rapid evolution of technology. SDV deployment has a substantial obstacle in requiring more exact and standardized regulations across various jurisdictions. The national rollout of self-driving vehicles (SDVs) is made more difficult by the wide range of regulatory requirements across the United States. For example, each state has its own guidelines regulating the testing and deployment of autonomous vehicles. The primary obstacle that the business must overcome is establishing a comprehensive legal framework that promotes innovation and guarantees the safety and dependability of these automobiles.

Explainability and Bias

Understanding how AI systems reach certain decisions might be challenging due to their inherent opacity. Particularly in mission-critical domains like autonomous driving, where choices might have fatal ramifications, the difficulty of AI algorithms' lack of explainability and the possibility of bias is enormous. To establish public confidence and guarantee the ethical deployment of SDVs, it is crucial to ensure that AI systems are open and impartial in their operations.

Computational Power and Resource Constraints

A vehicle's physical and energy limitations might limit the computational power needed to run the complicated artificial intelligence algorithms required for autonomous driving. Creating efficient and effective AI systems that meet these demands is a significant problem. Adding insult to injury, these systems must process and evaluate data in real-time so drivers can make split-second decisions.

Conclusions

This study aims to provide a thorough evaluation of the role that AI algorithms play in autonomous cars. Enhanced model capabilities and processing power are driving a shift away from rule-based systems and toward deep neural networks, which are highlighted in the study. It outlines the different needs necessary for automobiles and trucks, underlining that automobiles are more concerned with passenger comfort and urban adaptability, whilst trucks are more concerned with optimizing routes and maximizing fuel efficiency. The evolution of object detection from its most fundamental form to more complex forms like three-dimensional mapping and adaptive behaviour prediction is discussed. At higher degrees of autonomy, problems such as limited storage, processing power, software upgrades, and security holes become more apparent. Among the most crucial results is the emphasis on the importance of AI in developing various degrees of autonomy for cars. Deep learning and reinforcement learning are two examples of the cutting-edge methods needed to make complicated decisions. Since the software package grows in size with increasing levels of autonomy, efficient designs and strong security measures are required. These steps are necessary since they cause problems with storage, processing, and updating. Even though

self-driving trucks have significant business potential, there is a pressing need for additional research on the subject to improve logistics and address driver shortages.

References

1. Bordoloi, U.; Chakraborty, S.; Jochim, M.; Joshi, P.; Raghuraman, A.; Ramesh, S. Autonomy-driven Emerging Directions in Software-defined Vehicles. In Proceedings of the 2023 Design, Automation & Test in Europe Conference & Exhibition (DATE), Antwerp, Belgium, 17–19 April 2023; pp. 1–6. [**Google Scholar**] [**CrossRef**]
2. Liu, Z.; Zhang, W.; Zhao, F. Impact, challenges and the prospect of software-defined vehicles. Automot. Innov. **2022**, 5, 180–194. [**Google Scholar**] [**CrossRef**]
3. Nadikattu, R.R. New ways in artificial intelligence. Int. J. Comput. Trends Technol. **2019**, 67. [**Google Scholar**] [**CrossRef**]
4. Deng, Z.; Yang, K.; Shen, W.; Shi, Y. Cooperative Platoon Formation of Connected and Autonomous Vehicles: Toward Efficient Merging Coordination at Unsignalized Intersections. IEEE Trans. Intell. Transp. Syst. **2023**, 24, 5625–5639. [**Google Scholar**] [**CrossRef**]
5. Pugliese, A.; Regondi, S.; Marini, R. Machine Learning-based approach: Global trends, research directions, and regulatory standpoints. Data Sci. Manag. **2021**, 4, 19–29. [**Google Scholar**] [**CrossRef**]
6. SAE Industry Technologies Consortia's Automated Vehicle Safety Consortium AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon, AVSC00002202004, Revised April, 2020. Available online: **https://www.sae.org/standards/content/avsc00002202004/** (accessed on 28 January 2024).
7. Khastgir, S.; Khastgir, S.; Vreeswijk, J.; Shladover, S.; Kulmala, R.; Alkim, T.; Wijbenga, A.; Maerivoet, S.; Kotilainen, I.; Kawashima, K.; et al. Distributed ODD Awareness for Connected and Automated Driving. Transp. Res. Procedia **2023**, 72, 3118–3125. [**Google Scholar**] [**CrossRef**]
8. Jack, W.; Jon, B. Navigating Tomorrow: Advancements and Road Ahead in AI for Autonomous Vehicles; (No. 11955); EasyChair: Manchester, UK, 2024. [**Google Scholar**]
9. Lillo, L.D.; Gode, T.; Zhou, X.; Atzei, M.; Chen, R.; Victor, T. Comparative safety performance of autonomous-and human drivers: A real-world case study of the waymo one service. arXiv **2023**, arXiv:2309.01206. [**Google Scholar**]
10. Nordhoff, S.; Lee, J.D.; Hagenzieker, M.; Happee, R. (Mis-) use of standard Autopilot and Full Self-Driving (FSD) Beta: Results from interviews with users of Tesla's FSD Beta. Front. Psychol. **2023**, 14, 1101520. [**Google Scholar**] [**CrossRef**]
11. Wansley, M.T. Regulating Driving Automation Safety. Emory Law J. **2024**, 73, 505. [**Google Scholar**]
12. Anton, K.; Oleg, K. MBSE and Safety Lifecycle of AI-enabled systems in transportation. Int. J. Open Inf. Technol. **2023**, 11, 100–104. [**Google Scholar**]
13. Kang, H.; Lee, Y.; Jeong, H.; Park, G.; Yun, I. Applying the operational design domain concept to vehicles equipped with advanced driver assistance systems for enhanced safety. J. Adv. Transp. **2023**, 2023, 4640069
14. Vishnukumar, H.; Butting, B.; Müller, C.; Sax, E. Machine Learning and deep neural network—Artificial intelligence core for lab and real-world test and validation for ADAS and autonomous vehicles: AI for efficient and quality test and validation. In Proceedings of the 2017 Intelligent Systems Conference (IntelliSys), London, UK, 7–8 September 2017; pp. 714–721. [**Google Scholar**]
15. Bachute, M.R.; Subhedar, J.M. Autonomous driving architectures: Insights of machine Learning and deep Learning algorithms. Mach. Learn. Appl. **2021**, 6, 00164. [**Google Scholar**] [**CrossRef**]
16. Ma, Y.; Wang, Z.; Yang, H.; Yang, L. Artificial intelligence applications in the development of autonomous vehicles: A survey. IEEE/CAA J. Autom. Sin. **2020**, 7, 315–329. [**Google Scholar**] [**CrossRef**]
17. Bendiab, G.; Hameurlaine, A.; Germanos, G.; Kolokotronis, N.; Shiaeles, S. Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. IEEE Trans. Intell. Transp. Syst. **2023**, 24, 3614–3637. [**Google Scholar**] [**CrossRef**]
18. Chu, M.; Zong, K.; Shu, X.; Gong, J.; Lu, Z.; Guo, K.; Dai, X.; Zhou, G. Work with AI and Work for AI: Autonomous Vehicle Safety Drivers' Lived Experiences. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, Hamburg, Germany, 23–28 April 2023; pp. 1–16. [**Google Scholar**]
19. Hwang, M.H.; Lee, G.S.; Kim, E.; Kim, H.W.; Yoon, S.; Talluri, T.; Cha, H.R. Regenerative braking control strategy based on AI algorithm to improve driving comfort of autonomous vehicles. Appl. Sci. **2023**, 13, 946