Volume 5, Issue 2, 2022

Peer-reviewed, open-access journal dedicated to publishing high-quality research on sustainable technology and infrastructure in developing countries.

https://research.tensorgate.org/index.php/tjstidc

An Overview of Security and Privacy Challenges in Connected Autonomous Vehicles

Hadeel Ahmad Abu Ghazaleh

Al-Zaytoonah University of Jordan

ABSTRACT

The emergence of connected autonomous vehicles (CAVs) is transforming the way we travel and transport goods. However, as with any new technology, there are significant security and privacy challenges that must be addressed to ensure their safe and widespread adoption. This research study provides an overview of the key security and privacy challenges facing CAVs. One of the most pressing challenges is cybersecurity. CAVs rely heavily on communication networks to exchange data with other vehicles, infrastructure, and the cloud. This makes them vulnerable to cyberattacks, which could compromise the safety of passengers and other road users. Cybersecurity risks include theft of sensitive data, unauthorized access to vehicle controls, and hacking of sensors and communication systems.Data privacy is another significant challenge. CAVs generate and collect a large amount of data about their surroundings and occupants. This data could be used to track people's movements and habits, and to infer sensitive information such as health status or financial situation. Ensuring that this data is collected and stored securely and used only for its intended purposes is crucial for protecting the privacy of CAV users. As CAVs become more widespread, questions about liability in the event of an accident will become more pressing. Resolving these questions will be crucial for establishing a legal framework that can support the safe and responsible use of CAVs. Human-machine interaction is another challenge facing CAVs. CAVs rely on complex algorithms and machine learning models to make decisions about how to navigate the road.These algorithms can be opaque and difficult for humans to understand, which can create a sense of mistrust and unease. Ensuring that users have a clear understanding of how CAVs work and how to interact with them safely will be crucial for ensuring their adoption. CAVs are physical objects that can be targeted by physical attacks, such as vandalism or theft. Ensuring that CAVs are designed and built with physical security in mind will be crucial for ensuring their long-term viability.CAVs are complex systems that require a range of components, including sensors, processors, and communication modules. Ensuring the security of these components throughout the supply chain is crucial for protecting the overall security of the vehicle.

Keywords: *Connected Autonomous Vehicles, CAVs, Security, Privacy, Cybersecurity, Data Privacy*

INTRODUCTION

Connected autonomous vehicles (CAVs) have the potential to revolutionize the way we travel and transport goods, providing a safer, more efficient, and more sustainable alternative to traditional modes of transportation. By leveraging advanced technologies such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT), CAVs are designed to operate without human intervention, making them faster, more reliable, and more cost-effective than traditional vehicles.

As with any new technology, CAVs present significant security and privacy challenges that must be addressed to ensure their widespread adoption and safe use. From cyber attacks to data privacy concerns, from liability questions to human-machine interaction issues, there are a range of complex challenges that must be overcome if CAVs are to reach their full potential.

One of the most significant security challenges facing CAVs is cybersecurity. Because CAVs rely heavily on communication networks to exchange data with other vehicles, infrastructure, and the cloud, they are vulnerable to cyber attacks that could compromise the safety of passengers and other road users. Cybersecurity risks associated with CAVs include theft of sensitive data, unauthorized access to vehicle controls, and hacking of sensors and communication systems. Addressing these risks will require the development of robust cybersecurity protocols that can effectively protect CAVs from cyber threats.

CAVs also generate and collect a vast amount of data about their surroundings and their occupants. This data could be used to track people's movements and habits, and to infer sensitive information such as health status or financial situation. Ensuring that this data is collected and stored securely and used only for its intended purposes is crucial for protecting the privacy of CAV users. Therefore, data privacy must be a top priority for manufacturers and policymakers.As CAVs become more widespread, questions about liability in the event of an accident will become more pressing. For instance, who is responsible if a CAV crashes due to a software malfunction? Is it the manufacturer, the software developer, or the user? Resolving these questions will be crucial for establishing a legal framework that can support the safe and responsible use of CAVs.

CAVs rely on complex algorithms and machine learning models to make decisions about how to navigate the road. However, these algorithms can be opaque and difficult for humans to understand, which can create a sense of mistrust and unease. Ensuring that users have a clear understanding of how CAVs work and how to interact with them safely will be crucial for ensuring their adoption.As physical objects, CAVs can be targeted by physical attacks, such as vandalism or theft. Ensuring that CAVs are designed and built with physical security in mind will be crucial for ensuring their long-term viability.

Supply chain security is also a significant challenge facing CAVs. CAVs are complex systems that require a range of components, including sensors, processors, and communication modules. Ensuring the security of these components throughout the supply chain is crucial for protecting the overall security of the vehicle. Weaknesses in any of the components could be exploited by attackers to compromise the entire system. As a result, manufacturers need to ensure that their supply chain partners have robust security protocols in place and that they are following best practices for securing their systems.

While CAVs offer many benefits, they also present significant security and privacy challenges that must be addressed in order to ensure their widespread adoption and safe use. Cybersecurity, data privacy, liability, human-machine interaction, physical security, and supply chain security are all areas that require attention. Addressing these challenges will require a multifaceted approach involving collaboration between policymakers, manufacturers, users, and the research and development community. By working together to develop and implement robust security and privacy protocols, we can help to ensure that CAVs realize their full potential as a transformative technology for the transportation sector.

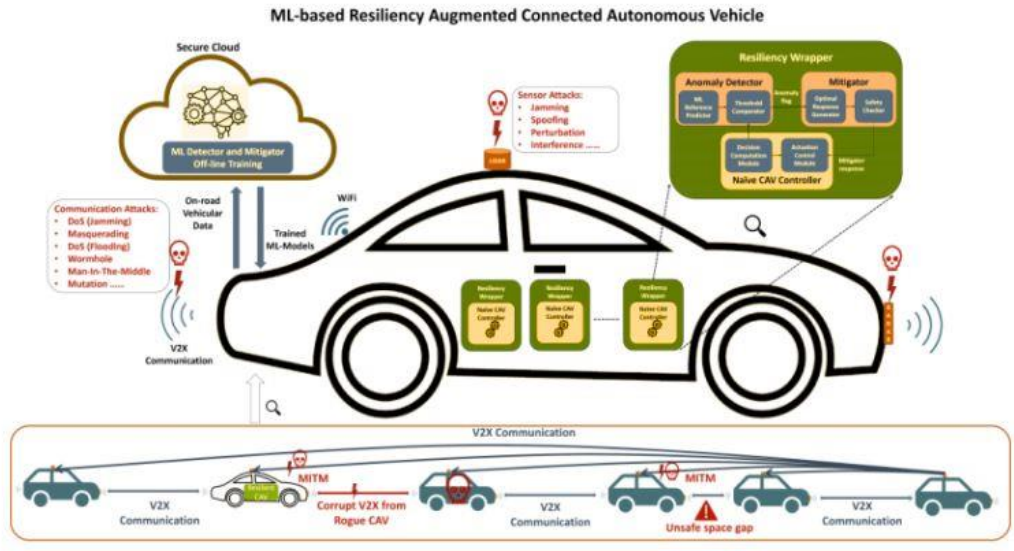

Figure 1- Connected Autonomous Vehicle system

Challenges

Cybersecurity:

The increasing reliance of connected autonomous vehicles (CAVs) on communication networks presents a significant challenge to cybersecurity. The constant exchange of data between vehicles, infrastructure, and the cloud makes these systems highly vulnerable to cyberattacks. One of the most pressing concerns is the potential compromise of passenger safety and that of other road users. In the event of a successful cyberattack, attackers could gain unauthorized access to vehicle controls, thereby compromising the functionality of the vehicle and posing a risk to all involved. This could result in severe physical harm and even loss of life.

The risks associated with cybersecurity in CAVs extend beyond physical harm to the theft of sensitive data. Cyber attackers could potentially gain access to valuable data that CAVs collect during their operations. This data may include personally identifiable information, GPS coordinates, and other sensitive information. The impact of such a breach could be far-reaching and potentially lead to identity theft and financial fraud.With the advent of smart cities and connected infrastructure, attackers could compromise the entire ecosystem by gaining access to critical infrastructure and disabling vital services.

Hacking of sensors and communication systems is yet another cybersecurity risk that CAVs face. Sensors play a critical role in enabling CAVs to detect and respond to their environment.A successful cyberattack could compromise the functionality of these sensors, leading to incorrect and potentially hazardous responses. Additionally, hackers could exploit communication systems and introduce false data or manipulate existing data, leading to misinterpretation by the vehicle's control system. In both cases, the consequences could be severe, leading to physical harm and loss of life.

As CAVs continue to evolve, cybersecurity risks will persist. The use of artificial intelligence and machine learning in these systems presents new vulnerabilities, which attackers can exploit.There is no doubt that these technologies hold immense potential to revolutionize the transportation industry. The challenge for policymakers and the industry will be to ensure that robust cybersecurity measures are in place to mitigate the risks associated with the use of CAVs. As cybersecurity threats continue to evolve, it is crucial that CAV developers remain vigilant and adopt a proactive approach to security.

The rise of connected autonomous vehicles presents new and significant cybersecurity challenges. With the ever-increasing reliance on communication networks and sensors, CAVs are highly vulnerable to cyberattacks. The risks associated with these attacks range from physical harm to the theft of sensitive data and hacking of critical infrastructure. As such, it is essential that policymakers and the industry take a proactive approach to cybersecurity and develop robust measures to mitigate the risks. By doing so, we can ensure that CAVs fulfill their potential to revolutionize the transportation industry without compromising the safety and security of passengers and other road users.

Data privacy:

Connected autonomous vehicles (CAVs) generate and collect vast amounts of data that have the potential to reveal sensitive information about their occupants and their surroundings. This data includes information about passengers' movements, habits, and even health status or financial situation. Protecting the privacy of CAV users is of utmost importance, and ensuring that this data is collected, stored, and used securely and only for its intended purposes is crucial.The vast amount of data collected by CAVs presents unique privacy concerns. The data could be used to track individuals' movements and activities, which could reveal a wealth of information about their personal lives. For instance, a person's regular travel route may indicate their place of work or frequent social activities. Similarly, data about a person's health status could be used to infer sensitive information about their physical and mental health. This data could be misused for malicious purposes, such as identity theft or discrimination in employment or insurance.

The collection and storage of personal data raise concerns about data breaches and unauthorized access. The data collected by CAVs is valuable and could be a prime target for cyber attackers. If the data falls into the wrong hands, the consequences could be severe, leading to identity theft, fraud, or even physical harm. It is, therefore, essential that the data collected by CAVs is encrypted and stored securely to minimize the risks of data breaches and unauthorized access.Ensuring that the data collected by CAVs is used only for its intended purposes is also critical for protecting users' privacy. This requires clear and transparent policies on data collection and use. CAV manufacturers and service providers must be transparent about the data collected and provide users with clear choices on how their data is used. Users must be able to opt-in or out of data collection and be informed about the purposes for which their data is used. Additionally, data should be anonymized whenever possible to minimize the risks of data misuse.

Protecting the privacy of CAV users is crucial, given the vast amount of data generated and collected by these vehicles. The data could reveal sensitive information about individuals, and if misused, could result in severe consequences. To ensure that users' privacy is

protected, data must be collected, stored, and used securely and only for its intended purposes. Clear and transparent policies on data collection and use must be in place, and users must be given clear choices on how their data is used. By taking these measures, we can ensure that CAVs fulfill their potential to revolutionize the transportation industry without compromising users' privacy.

Liability:

As the deployment of Connected and Automated Vehicles (CAVs) grows, it has become increasingly clear that liability is one of the most critical concerns that need to be addressed. With the advent of sophisticated software that controls a car's every move, it has become more complicated to determine who is responsible in the event of an accident. Is it the car manufacturer, the software developer, or the user? This question has sparked a lot of debate and will continue to do so until a satisfactory answer is found. The legal framework that governs the use of CAVs must be capable of addressing this issue, as it is crucial for establishing safe and responsible use.

The issue of liability in the event of a CAV crash due to a software malfunction is complex. When a person is driving a car, they are liable for any accidents that occur.When it comes to CAVs, it is not clear who is responsible for a software malfunction. Is it the manufacturer of the car who is responsible for the software, the software developer who created the code, or the user who is driving the car? This question has significant implications for the legal framework that governs the use of CAVs.The lack of clarity regarding liability in the event of an accident involving a CAV can have serious consequences. If manufacturers are held liable for accidents caused by software malfunctions, they may become hesitant to develop new CAV technology. On the other hand, if the user is held responsible, it could deter people from using CAVs altogether. To ensure that the use of CAVs is safe and responsible, it is essential to establish a legal framework that addresses these liability issues.

The resolution of liability questions surrounding CAVs is vital to ensure that the transition to this technology is smooth and safe. It is not enough to rely on traditional legal frameworks, as they may not be equipped to handle the complexities that arise with the use of CAVs. To address these issues, a new legal framework needs to be developed that is capable of holding all parties responsible for any accidents caused by CAVs. This framework should also incentivize manufacturers and developers to create safe and reliable software for CAVs, which will ultimately help to make the use of these vehicles more secure.

As CAVs become more widespread, questions of liability in the event of an accident will become more pressing. Resolving these issues is essential for establishing a legal framework that can support the safe and responsible use of CAVs. The lack of clarity regarding liability in the event of a software malfunction can have serious consequences, which could ultimately undermine the adoption of CAVs.A new legal framework needs to be developed that is capable of holding all parties responsible for any accidents caused by CAVs. This framework should incentivize manufacturers and developers to create safe and reliable software for CAVs and help make the use of these vehicles more secure.

Human-machine interaction:

Human-machine interaction has been a crucial topic of discussion in recent years. With the advent of autonomous and connected vehicles (CAVs), it has become more important than ever to ensure that users have a clear understanding of how these technologies work and how to interact with them safely. CAVs rely on complex algorithms and machine learning models to make decisions about how to navigate the road. While these algorithms are highly sophisticated, they can also be opaque and difficult for humans to understand. This can create a sense of mistrust and unease, which could ultimately impede the adoption of these technologies.

CAV manufacturers must ensure that users have access to clear and concise information about how these technologies work, what their limitations are, and how to interact with them safely. This could involve providing detailed user manuals, instructional videos, or even interactive training programs. By empowering users with this knowledge, they will be better equipped to understand and trust the decisions made by CAVs, which will ultimately increase their adoption.Effective human-machine interaction also requires a deep understanding of human behavior and psychology. CAVs must be designed with the human user in mind, taking into account their cognitive processes, emotions, and decision-making patterns. This means designing interfaces that are intuitive and easy to use, minimizing distractions and cognitive load, and providing clear feedback to users. By aligning the design of CAVs with human behavior, we can ensure that these technologies are as user-friendly and accessible as possible.

Achieving effective human-machine interaction is not without its challenges. As CAVs become more advanced, they are likely to encounter increasingly complex situations on the road. This could include unexpected obstacles, adverse weather conditions, or even other drivers who are behaving erratically. In these situations, it will be crucial for CAVs to communicate effectively with their human passengers, explaining their decision-making processes and providing clear guidance on how to stay safe. Achieving this level of communication will require ongoing research and development in the field of human-machine interaction.

Human-machine interaction is a critical factor in the adoption of CAVs. To ensure that these technologies are embraced by users, it is essential to prioritize transparency, education, and user-centered design. This will require ongoing research and development in the field of human-machine interaction, as well as collaboration between CAV manufacturers, regulators, and other stakeholders. By working together, we can create a future in which CAVs are not only safe and efficient but also accessible and intuitive for all users.

Physical security:

As autonomous vehicles become more common, they will likely become attractive targets for physical attacks such as vandalism or theft. These attacks can have serious consequences, not only for the owners of the vehicles but also for the safety of other road users. Ensuring that CAVs are designed and built with physical security in mind will be crucial for ensuring their long-term viability.

Physical security for CAVs involves a range of measures that can be taken to prevent physical attacks. These measures can include the use of tamper-resistant components, secure communication protocols, and physical barriers such as fences or bollards. Additionally, CAVs can be equipped with sensors and alarms that can detect and alert owners or authorities to any attempted attacks. By incorporating these measures into the design of CAVs, manufacturers can reduce the likelihood of successful physical attacks and increase the overall security of the vehicles.

One of the challenges of ensuring physical security for CAVs is the fact that they will be operating in public spaces, where they will be exposed to a wide range of potential threats. This means that physical security measures must be designed to be robust and resilient, able to withstand a range of different attacks. Additionally, manufacturers must consider the potential for attacks from insiders, such as employees or contractors, who may have access to sensitive components or information.Another important consideration for physical security of CAVs is the potential for attacks on the supporting infrastructure, such as charging stations or traffic management systems. These attacks could have serious consequences for the operation of CAVs, potentially disrupting entire networks of vehicles. To prevent such attacks, it will be important to ensure that the supporting infrastructure is designed and built with physical security in mind, and that appropriate measures are taken to monitor and secure these systems.

Physical security is a critical component of the long-term viability of CAVs. As these vehicles become more common, they will become increasingly attractive targets for physical attacks, which could have serious consequences for their owners and for other road users. Ensuring that CAVs are designed and built with physical security in mind will require a range of measures, from tamper-resistant components to secure communication protocols and physical barriers. By taking these measures, manufacturers can reduce the likelihood of successful physical attacks and increase the overall security of CAVs and the infrastructure that supports them.

Supply chain security:

The complexity of connected autonomous vehicles (CAVs) requires a range of components, including sensors, processors, and communication modules. These components must function seamlessly together to ensure that the CAV operates safely and efficiently. However, with this complexity comes an increased risk of security breaches. The supply chain is an integral part of the CAV ecosystem, and securing it is essential to ensure the overall security of the vehicle. The supply chain includes everything from the sourcing of raw materials to the manufacturing and assembly of components, and even the delivery of finished vehicles to dealerships. Each step in the supply chain must be secure to prevent attackers from exploiting any weaknesses and compromising the entire system. Manufacturers must therefore work closely with their supply chain partners to ensure that security is a top priority and that best practices are being followed.

The security of the CAV supply chain must be approached holistically, with an understanding that any weakness in the system could have catastrophic consequences. Manufacturers must work to identify potential vulnerabilities at every step in the supply chain and develop strategies to mitigate these risks. This includes ensuring that all

components are sourced from trusted suppliers with robust security protocols in place, and that all personnel involved in the supply chain have undergone thorough background checks. Manufacturers must also work to ensure that all software and firmware components are properly updated and patched to address any known vulnerabilities. By taking a comprehensive approach to supply chain security, manufacturers can help ensure that CAVs are as safe and secure as possible.

One of the most significant challenges in securing the CAV supply chain is the sheer number of suppliers involved. CAVs require a vast array of components, and each of these components may come from a different supplier, making it challenging to track and secure every aspect of the supply chain. This challenge is compounded by the fact that many of these suppliers may be located in different countries and may have different security standards and protocols. Manufacturers must, therefore, work closely with their suppliers to ensure that all security requirements are met and that there is a consistent approach to security across the entire supply chain. This requires a significant investment of time and resources but is essential to ensure the overall security of the CAV.

As new threats emerge, manufacturers must work quickly to identify and address any vulnerabilities in their supply chain. This requires a proactive approach to security, with regular audits and risk assessments conducted to identify potential areas of weakness. Manufacturers must also work closely with their suppliers to ensure that all security updates and patches are applied in a timely manner. This ongoing effort requires a significant investment of time and resources, but it is essential to ensure that CAVs remain secure and that any potential security breaches are quickly identified and addressed.

Supply chain security is a critical aspect of CAV development and deployment. Manufacturers must take a comprehensive approach to security, working closely with their suppliers to ensure that all components and processes are secure and that best practices are being followed. This requires a significant investment of time and resources, but it is essential to ensure the overall security of the CAV. By taking a proactive approach to security, regularly assessing and updating security protocols, and working closely with suppliers, manufacturers can help ensure that CAVs are as safe and secure as possible.

CONCLUSION

Connected autonomous vehicles (CAVs) present significant security and privacy challenges that must be addressed to ensure their widespread adoption and safe use. These challenges include cybersecurity, data privacy, liability, human-machine interaction, physical security, and supply chain security. While CAVs offer numerous benefits, such as increased safety and efficiency, they also pose unique risks that must be addressed to realize their full potential. Policymakers will need to develop and enforce regulations that ensure the security and privacy of CAV users. Manufacturers will need to design and build CAVs with security and privacy in mind, and ensure that their supply chain partners are following best practices for securing their systems. Users will need to be educated on how to interact with CAVs safely and responsibly.

Developing robust cybersecurity protocols will be crucial for protecting CAVs against cyberattacks that could compromise their safety and security. Ensuring data privacy will be crucial for protecting the privacy of CAV users and preventing the misuse of their personal information. Establishing liability frameworks will be crucial for resolving questions about responsibility in the event of an accident. Improving human-machine interaction will be crucial for ensuring that users have a clear understanding of how CAVs work and how to interact with them safely. Enhancing physical security will be crucial for protecting CAVs against physical attacks, such as vandalism or theft.

Addressing the security and privacy challenges in CAVs will require a coordinated effort from all stakeholders. While these challenges may seem daunting, they can be overcome with careful planning, collaboration, and innovation. By working together, policymakers, manufacturers, and users can ensure the safe and responsible use of CAVs and unlock their full potential for transforming the way we travel and transport goods.

REFERENCES

[1] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[2] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[3] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, Jan. 2019.

[4] T. Litman, *Autonomous vehicle implementation predictions*. Victoria Transport Policy Institute Victoria, BC, Canada, 2017.

[5] P. Uyyala, "DETECTING AND CHARACTERIZING EXTREMIST REVIEWER GROUPS IN ONLINE PRODUCT REVIEWS," *Journal of interdisciplinary cycle research*, vol. 14, no. 4, pp. 1689–1699, 2022.

[6] R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1275–1313, Secondquarter 2019.

[7] B. Schoettle and M. Sivak, "A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia," University of Michigan, Ann Arbor, Transportation Research Institute, 2014.

[8] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies," *Journal of Modern Transportation*, vol. 24, no. 4, pp. 284–303, Dec. 2016.

[9] A. K. Venkitaraman and V. S. R. Kosuru, "Electric Vehicle Charging Network Optimization using Multi-Variable Linear Programming and Bayesian Principles," in *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, 2022, pp. 1–5.

[10] P. Uyyala, "AUTOMATIC DETECTION OF GENETIC DISEASES IN PEDIATRIC AGE USING PUPILLOMETRY," *Journal of interdisciplinary cycle research*, vol. 14, no. 5, pp. 1748–1760, 2022.

[11] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 241–246.
[12] P. Uyyala, "DETECTION OF CYBER ATTACK IN NETWORK USING MACHINE LEARNING TECHNIQUES," *Journal of interdisciplinary cycle research*, vol. 14, no. 3, pp. 1903–1913, 2022.
[13] M. Kyriakidis, R. Happee, and J. C. F. de Winter, "Public opinion on automated driving: Results of an international questionnaire among 5000 respondents," *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 32, pp. 127–140, Jul. 2015.
[14] V. S. Rahul, "Kosuru; Venkitaraman, AK Integrated framework to identify fault in human-machine interaction systems," *Int. Res. J. Mod. Eng. Technol. Sci*, 2022.
[15] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016, pp. 164–170.
[16] D. Lee and D. J. Hess, "Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization," *Transp. Res. Part A: Policy Pract.*, vol. 136, pp. 85–98, Jun. 2020.
[17] M. Hengstler, E. Enkel, and S. Duelli, "Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices," *Technol. Forecast. Soc. Change*, vol. 105, pp. 105–120, Apr. 2016.
[18] P. Bansal and K. M. Kockelman, "Forecasting Americans' long-term adoption of connected and autonomous vehicle technologies," *Transp. Res. Part A: Policy Pract.*, vol. 95, pp. 49–63, Jan. 2017.
[19] P. Uyyala, "SECURE CRYPTO-BIOMETRIC SYSTEM FOR CLOUD COMPUTING," *Journal of interdisciplinary cycle research*, vol. 14, no. 6, pp. 2344–2352, 2022.
[20] S. Kuutti, S. Fallah, K. Katsaros, and M. Dianati, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of*, 2018.
[21] V. S. R. Kosuru and A. K. Venkitaraman, "Developing a deep Q-learning and neural network framework for trajectory planning," *European Journal of Engineering and Technology Research*, vol. 7, no. 6, pp. 148–157, Dec. 2022.
[22] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 22–28, Mar. 2017.
[23] R. Krajewski, J. Bock, L. Kloeker, and L. Eckstein, "The highD Dataset: A Drone Dataset of Naturalistic Vehicle Trajectories on German Highways for Validation of Highly Automated Driving Systems," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 2118–2125.
[24] P. Uyyala, "PREDICTING RAINFALL USING MACHINE LEARNING TECHNIQUES," *J. Interdiscipl. Cycle Res.*, vol. 14, no. 2, pp. 1284–1292, 2022.
[25] P. Uyyala, "Secure Channel Free Certificate-Based Searchable Encryption Withstanding Outside and Inside Keyword Guessing Attacks," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 2, pp. 2467–2474, 2021.
[26] E. Schoitsch, C. Schmittner, Z. Ma, and T. Gruber, "The Need for Safety and Cyber-Security Co-engineering and Standardization for Highly Automated Automotive

Vehicles," in *Advanced Microsystems for Automotive Applications 2015*, 2016, pp. 251–261.
[27] P. Uyyala, "Privacy-aware Personal Data Storage (P-PDS): Learning how toProtect User Privacy from External Applications," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 6, pp. 3257–3273, 2021.
[28] C. Gkartzonikas and K. Gkritza, "What have we learned? A review of stated preference and choice studies on autonomous vehicles," *Transp. Res. Part C: Emerg. Technol.*, vol. 98, pp. 323–337, Jan. 2019.
[29] P. Uyyala, "COLLUSION DEFENDER PRESERVING SUBSCRIBERS PRIVACY IN PUBLISH AND SUBSCRIBE SYSTEMS," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 4, pp. 2639–2645, 2021.
[30] I. Panagiotopoulos and G. Dimitrakopoulos, "An empirical investigation on consumers' intentions towards autonomous driving," *Transp. Res. Part C: Emerg. Technol.*, vol. 95, pp. 773–784, Oct. 2018.
[31] T. Zhang, D. Tao, X. Qu, X. Zhang, R. Lin, and W. Zhang, "The roles of initial trust and perceived risk in public's acceptance of automated vehicles," *Transp. Res. Part C: Emerg. Technol.*, vol. 98, pp. 207–220, Jan. 2019.
[32] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017.
[33] V. S. R. Kosuru, A. K. Venkitaraman, V. D. Chaudhari, N. Garg, A. Rao, and A. Deepak, "Automatic Identification of Vehicles in Traffic using Smart Cameras," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 2022, pp. 1009–1014.
[34] J.-F. Bonnefon *et al.*, *Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability and responsibility*. aaltodoc.aalto.fi, 2020.
[35] P. Seuwou, E. Banissi, and G. Ubakanma, "The Future of Mobility with Connected and Autonomous Vehicles in Smart Cities," in *Digital Twin Technologies and Smart Cities*, M. Farsi, A. Daneshkhah, A. Hosseinian-Far, and H. Jahankhani, Eds. Cham: Springer International Publishing, 2020, pp. 37–52.
[36] J. He *et al.*, "Cooperative Connected Autonomous Vehicles (CAV): Research, Applications and Challenges," in *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, 2019, pp. 1–6.
[37] F. Pütz, F. Murphy, M. Mullins, and L. O'Malley, "Connected automated vehicles and insurance: Analysing future market-structure from a business ecosystem perspective," *Technol. Soc.*, vol. 59, p. 101182, Nov. 2019.
[38] J.-F. Aguinaga, *Ethics of Connected and Automated Vehicles Recommendations on road safety, privacy, fairness, explainability and responsibility*. sicurstrada.it, 2020.
[39] A. K. Venkitaraman and V. S. R. Kosuru, "A review on autonomous electric vehicle communication networks-progress, methods and challenges," *World J. Adv. Res. Rev.*, vol. 16, no. 3, pp. 013–024, Dec. 2022.
[40] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach," *Transp. Res. Part F Traffic Psychol. Behav.*, vol. 75, pp. 66–86, Nov. 2020.
[41] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transp. Res. Part A: Policy Pract.*, vol. 124, pp. 523–536, Jun. 2019.
[42] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transp. Res. Part A: Policy Pract.*, vol. 77, pp. 167–181, Jul. 2015.

[43] T. Li, L. Lin, and S. Gong, "AutoMPC: Efficient Multi-Party Computation for Secure and Privacy-Preserving Cooperative Control of Connected Autonomous Vehicles," in *SafeAI@ AAAI*, 2019.
[44] I. Brass, M. Carr, L. Tanczer, C. Maple, and J. J. Blackstock, "Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles: Part I," *Autonomous Vehicles ...*, 04-May-2017.
[45] P. Uyyala, "Efficient and Deployable Click Fraud Detection for Mobile Applications," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 1, pp. 2360–2372, 2021.
[46] P. Uyyala, "Credit Card Transactions Data Adversarial Augmentation in the Frequency Domain," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 5, pp. 2712–2718, 2021.
[47] A. T. Sheik and C. Maple, "Key Security Challenges for Cloud-assisted Connected and Autonomous Vehicles," p. 17 (9 pp.)-17 (9 pp.), Jan. 2019.
[48] D. J. Hess, "Incumbent-led transitions and civil society: Autonomous vehicle policy and consumer organizations in the United States," *Technol. Forecast. Soc. Change*, vol. 151, p. 119825, Feb. 2020.
[49] P. Uyyala, "Delegated Authorization Framework for EHR Services using Attribute Based Encryption," *The International journal of analytical and experimental modal analysis*, vol. 13, no. 3, pp. 2447–2451, 2021.
[50] P. Uyyala, "SIGN LANGUAGE RECOGNITION USING CONVOLUTIONAL NEURAL NETWORKS," *Journal of interdisciplinary cycle research*, vol. 14, no. 1, pp. 1198–1207, 2022.
[51] M. Chowdhury, M. Islam, and Z. Khan, "Security of Connected and Automated Vehicles," *arXiv [cs.CR]*, 24-Dec-2020.
[52] A. Faisal, T. Yigitcanlar, M. Kamruzzaman, and G. Currie, "Understanding autonomous vehicles: A systematic literature review on capability, impact, planning and policy," *J. Transp. Land Use*, vol. 12, no. 1, pp. 45–72, Jan. 2019.
[53] S. Baker, C. M. Theissen, and B. Vakil, "Connected and autonomous vehicles: A cross-jurisdictional comparison of regulatory developments," *of Robotics, Artificial Intelligence & Law*, 2020.
[54] V. S. R. Kosuru and A. K. Venkitaraman, "Preventing the False Negatives of Vehicle Object Detection in Autonomous Driving Control Using Clear Object Filter Technique," in *2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, 2022, pp. 1–6.
[55] A. Dabboussi, "Dependability approaches for mobile environment: Application on connected autonomous vehicles," Université Bourgogne Franche-Comté, 2019.
[56] S. A. Cohen and D. Hopkins, "Autonomous vehicles and the future of urban tourism," *Ann. Touris. Res.*, vol. 74, pp. 33–42, Jan. 2019.
[57] I. Brass, L. Tanczer, C. Maple, J. J. Blackstock, and M. Carr, "Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles: Part II," *Autonomous Vehicles ...*, 04-May-2018.