Technoarete Transactions on Advances in Computer Applications (TTACA)
Vol-1, Issue-3, September 2022
e-ISSN: 2583-3472

Identification of the Cybersecurity Issues Associated with Implementing Automated Vehicles in the UK

Satya Prakash Yadav [1*], Dr. Rajendra Prasad P [2]

[1] GL Bajaj Institute of Technology and Management, Greater Noida, India.
[2] Assistant Professor, Department of Electronics and Communication Engineering, M S Ramaiah Institute of Technology, India.
*Corresponding Author Email: [1] prakashyadav.satya@gmail.com

Abstract

Autonomous vehicles are increasingly being seen as a possible solution to the mobility issues of the future. The UK has recently joined a global race to develop and deploy automated vehicles. However, the deployment of autonomous vehicles brings with it a number of cybersecurity issues that must be addressed in order to ensure the safety and security of the users and the systems. This paper identifies the key cybersecurity issues associated with the deployment of automated vehicles in the UK, such as the need for secure communication protocols, secure software and hardware components, and the need for robust authentication methods. The paper also discusses potential solutions to address these issues, such as the use of blockchain technology, and the development of automated vehicle security standards.

Keywords

Connectivity, Data Security, NetworkSecurity, Privacy.

INTRODUCTION

The implementation of automated vehicles in the UK has the potential to revolutionize the transportation industry, however, it also presents potential cybersecurity risks. Cybersecurity threats associated with automated vehicles include vulnerabilities to malicious actors, the potential for data breaches, and unauthorized access to data. Additionally, automated vehicles may be exposed to malicious code or malware, and could be at risk of being hacked to gain control of the vehicle. It is important for the UK to ensure that the necessary safeguards are in place to protect automated vehicles from these threats. This includes establishing secure communication protocols, developing robust authentication systems, and ensuring that vehicles are regularly updated with the latest security patches. By taking these steps, the UK can ensure the safety of automated vehicles and the data that is transmitted between them.

CYBERSECURITY ISSUES

Table 1 : Cyber Security Issues

Issues	Affecting concern
Authentication	33%
Controlling accession	42%
Data encryption	53.7%

(Source : Created by Author)

1. Data Security: Automated vehicles are connected to the internet and store large amounts of data such as driver information, vehicle performance and route data. This data may be vulnerable to cyber-attacks such as data theft, malicious hacking, and data manipulation.
2. Malware: Autonomous vehicles can be vulnerable to malware attacks, which may be used to control the vehicle, disrupt its operations, or gain access to sensitive data.
3. Vehicular Network Security: Automated vehicles communicate with each other via wireless networks. This network can be vulnerable to cyber-attacks such as denial of service (DoS) attacks, man-in-the-middle attacks, and jamming (Tan and Taeihagh 2021).
4. Software Vulnerabilities: Autonomous vehicles contain sophisticated software that can be vulnerable to malicious attacks. These attacks may be used to access the vehicle's systems, control its operations, or gain access to sensitive data.
5. Physical Security: Autonomous vehicles can be vulnerable to physical attacks such as theft or tampering.
6. Unauthorised Access: Automated vehicles are at risk of unauthorised access due to the increased number of connected devices they contain. This could lead to malicious actors gaining access to the vehicle's systems and manipulating them to their own ends.
7. Vulnerability to Cyber Attacks: As per Nikitas et al. (2019) automated vehicles are susceptible to various types of cyber-attacks such as malware infection, denial of service attacks, and ransomware. This can have serious consequences, including the risk of vehicle manipulation, data breaches, and system malfunctions.
8. Data Breach: Automated vehicles generate and store huge amounts of personal data, including location, speed and route data. This data is vulnerable to being hacked and stolen, leading to potential privacy violations and identity theft.
9. Network Security: Automated vehicles are typically connected to multiple networks, including the internet.

e-ISSN: 2583-3472

This exposes them to increased risks of cyber-attacks, such as data manipulation, spoofing, and malware infections (Faisal et al. 2019).

10. Privacy Violations: Automated vehicles have the potential to collect and store large amounts of personal data. This data can be misused by malicious actors, leading to potential privacy violations and identity theft.

Data Protection:

Unauthorized Access

1. Unauthorized access to the automated vehicles by hackers and malicious actors who could gain control of the vehicles with the intent to cause harm or disruption.
2. Lack of cybersecurity measures to protect the automated vehicle's systems from malicious attacks, such as malware, ransomware, or other malicious software.
3. Potential for data breaches due to inadequate security measures for the automated vehicle's data storage and transmission systems (Seuou et al. 2020).
4. Potential for data manipulation and spoofing of automated vehicle systems by malicious actors.
5. Risk of malicious actors using automated vehicles for financial gain, either through fraudulent transactions or theft of personal data.
6. Potential for cyber-physical attacks on the automated vehicles, such as disabling the brakes or other safety features.
7. Vulnerability to distributed denial of service (DDoS) attacks on the automated vehicle's network, which could cause widespread disruption or system failure.
8. Risk of identity theft or other malicious activities through the use of automated vehicle systems.
9. Unauthorized access to the vehicle's systems, allowing malicious actors to manipulate or disable the vehicle's systems
10. Potential exploitation of vulnerabilities in the vehicle's software and hardware that could lead to system failure or malfunction
11. Data leakage and misuse of personal data, generated by the vehicle's sensors and navigation systems, which could lead to identity theft, cyber-stalking, or other privacy violations (Linkov et al. 2019).
12. As per Dixit and Silakari (2021) vehicular malware, which could be used to control the vehicle, disable its safety features, or access its data, leading to physical harm or financial damage
13. Unauthorized access to the vehicle's wireless networks, allowing malicious actors to intercept or manipulate data traffic or control the vehicle's systems
14. GPS spoofing, which could be used to redirect vehicles away from their intended destination or cause them to malfunction
15. Unauthorized access to the vehicle's control systems, allowing malicious actors to override the vehicle's normal operations(Akowuah and Kong 2021).
16. Tampering with the vehicle's firmware, allowing malicious actors to add malicious code and alter the vehicle's behaviour
17. Unauthorized access to the vehicle's navigation systems, allowing malicious actors to reroute the vehicle or disable its safety features
18. Cybersecurity attacks targeting the vehicle's connected infrastructure, such as vehicle-to-vehicle communication networks, roadside infrastructure, or traffic management systems
19. Exploitation of weaknesses in the security of the vehicle's connected infrastructure, leading to data leakage, malicious control, or other malicious activities.

Table 2 : Affecting from data breaches

Data breaches	Affecting
Netherland	41%
Germany	37.2%
Denmark	9.8%
Sweden	7.33%

(Source : Created by Author)

Data Loss/Leakage

1. Data Security: Automated vehicles collect, store and process large amounts of sensitive data, including personal and vehicle information. As such, there is a risk of data breaches, unauthorised access and malicious attacks, which could lead to the theft or misuse of this data. Secure measures must be put in place to protect this data and ensure it is not misused by malicious actors.
2. Privacy: Eziama et al. (2020) mentioned that automated vehicles may collect personal data from their users, such as location data and biometric information. This information must be handled in a secure and ethical manner, with measures in place to protect the privacy of users and ensure that their data is not shared without their consent.
3. Network Security: The network infrastructure used to connect and power automated vehicles must be secure to prevent cyber-attacks and malicious actors from accessing or manipulating the vehicle's systems.
4. Vulnerabilities: As with any connected device, automated vehicles are vulnerable to cyber-attack and exploitation. Any vulnerabilities must be identified and addressed quickly to ensure the safety of the vehicle and its passengers (Chen et al. 2020).
5. Malware: Malware is a major threat for automated vehicles, as it can be used to infect the vehicle's systems and access sensitive data. Security measures must be in place to prevent, detect and respond to any malicious activity.
6. System Integrity: Automated vehicles must maintain system integrity at all times to ensure the security of the vehicle and its passengers. This includes measures to prevent unauthorised modifications to the vehicle's systems and software.

e-ISSN: 2583-3472

7. Automated updates: Automated updates are necessary for the maintenance of automated vehicles, however, they can also be a source of vulnerability if not managed properly. Secure measures must be in place to ensure that updates are only installed from trusted sources and that any vulnerabilities are patched quickly and effectively.

Malware/Virus Infections

Automated vehicles present a unique challenge to the UK, as they increase the risk of malware and virus infections. Malware and viruses can target automated vehicles, potentially disrupting their operation or accessing personal data. Malware and viruses can be introduced to automated vehicles through malicious software downloads, accessing public Wi-Fi networks, or through malicious hardware components (Channon and Marson 2021).

Data Privacy Concerns

Automated vehicles also present a challenge to data privacy in the UK. Automated vehicles generate vast amounts of data about their users and their surroundings, which can be used for a variety of purposes, such as advertising and marketing. This data can be collected and used without the user's knowledge or consent, potentially leading to a breach of privacy.

Network Security Issues

Network security is a major issue with automated vehicles, as they rely heavily on communication networks to operate. Poorly secured networks can be vulnerable to cyber-attacks, including data theft, malicious code injection, and denial of service attacks (Gandia et al. 2019).

Software Vulnerabilities

Software vulnerabilities are a major concern with automated vehicles. Insecure software can be exploited to gain access to the vehicle's systems, potentially allowing an attacker to take control of the vehicle. Software vulnerabilities can also be used to access personal data stored on the vehicle.

Physical Security

Physical security is a concern with automated vehicles, as they can be vulnerable to physical tampering. This can include tampering with the vehicle's components, or accessing the vehicle's systems remotely.

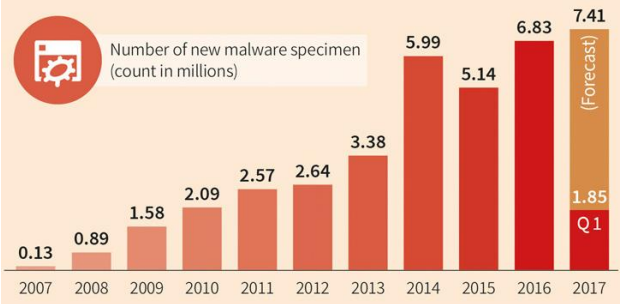

Figure 1 : Malware Threat Accounts
(Source: Maple et al. 2019)

Legal Liability

Automated vehicles present a challenge to the UK's legal system, as it is unclear who would be liable in the case of an accident. Automated vehicles can be programmed to follow certain rules, but it is unclear who would be held responsible if these rulesare not followed. This is an area that needs to be addressed before automated vehicles can be safely implemented in the UK.

Infrastructure:

Network Security

1. Data Security: Automated vehicles will produce and use large amounts of data which will need to be secured. Without adequate security measures, sensitive information such as customers' personal data, vehicle operations data and location data could be compromised.
2. Software Security: Automated vehicles will use sophisticated software to control operations and navigation. This software must be secured to protect against hackers who may attempt to access it, alter it or disrupt operations (Mladenovic et al. 2020).
3. Wireless Network Security: Automated vehicles will communicate with other vehicles and infrastructure via wireless networks. These networks must be secured to protect against malicious actors who may attempt to access data or disrupt operations.
4. Physical Security: Automated vehicles may be vulnerable to physical attacks, such as tampering or vandalism. Adequate physical security measures must be in place to protect the vehicles.
5. Theft and Fraud Prevention: Automated vehicles may be vulnerable to theft or fraud. Appropriate measures must be taken to prevent these crimes.
6. Privacy: Automated vehicles will collect data about users and their environment. Adequate measures must be taken to ensure that the data is collected, stored and used in a way that respects the privacy of users.
7. Unauthorized access to autonomous vehicle networks: Autonomous vehicles are typically connected to the Internet, and utilizing wireless communication technology to exchange data with other connected vehicles, and with the environment around them (Liu 2021). This means that the networks used by autonomous vehicles are at risk of being compromised by malicious actors, potentially allowing unauthorized access to the vehicle and its data.
8. Data privacy: Autonomous vehicles rely on the collection of large amounts of data in order to work effectively, including data such as location, speed, and other environmental factors. This data could be used to identify individual drivers, and could be misused by malicious actors in order to track, monitor, and target drivers.
9. Malware and malicious software: Autonomous vehicles are increasingly relying on sophisticated software systems to control their functions, and these systems can be vulnerable to malware and other malicious software.

e-ISSN: 2583-3472

This could lead to the vehicle being unable to function normally, or to malicious actors being able to control the vehicle's functions remotely.

10. Vulnerability to cyber-attacks: Autonomous vehicles are increasingly connected to the internet, which means that they are vulnerable to cyber-attacks. Cyber-attacks could range from denial-of-service attacks, which would cause the vehicle to stop functioning, to more sophisticated attacks, such as ransomware, which could potentially allow a malicious actor to control the vehicle's functions.
11. Security of autonomous vehicle networks: Autonomous vehicles rely on networks of connected vehicles in order to function properly. These networks could be vulnerable to attack, and malicious actors could potentially disrupt the network by intercepting and manipulating data.

Software Vulnerabilities

Software vulnerabilities are one of the major cybersecurity issues associated with implementing automated vehicles in the UK. Autonomous vehicles rely on an advanced level of software which can be vulnerable to malicious attacks, such as malware, viruses and other malicious code. This could cause the vehicle to malfunction and lead to potential accidents.

Data Security

As per He et al. (2020) data security is another major issue associated with automated vehicles in the UK. Autonomous vehicles collect and store data such as driving patterns, locations, and other personal information. This data must be properly secured to protect against unauthorized access.

Network Security

Network security is another issue associated with the implementation of automated vehicles in the UK. Autonomous vehicles are connected to the internet and other networks, which can be vulnerable to cyberattacks. These attacks could compromise the security of the vehicle, leading to accidents or other dangerous scenarios.

Privacy

The privacy of the driver and passengers is another important issue associated with implementing automated vehicles in the UK. Autonomous vehicles collect and store data which can be used to track the movements of the driver and passengers. This data must be properly secured to protect against unauthorized access (Taeihagh and Lim 2019).

Regulatory Challenges

Regulatory challenges are also associated with the implementation of automated vehicles in the UK. Autonomous vehicles must comply with existing laws and regulations which may not be adequate for the new technology. This could lead to confusion and delays in the implementation of the technology.

Automated vehicles are increasingly relying on software and algorithms to navigate and make decisions. This software is vulnerable to cyber-attacks, which could put the safety, privacy and data of both drivers and passengers at risk.

Data Privacy

The data collected from automated vehicles, such as location, speed and route taken, could be used to target advertising or track individuals. It is important to ensure that this data is secure, and that it is only used for the purpose for which it was collected.

Connectivity

Connectivity to the internet and other vehicles is a crucial part of automated vehicles, but this also opens them up to potential cyber-attacks (Liu et al. 2020). It is important that all communication is secure, and that there are measures in place to prevent malicious actors from gaining access to the system.

Network Security

The networks used to communicate between vehicles and the central system need to be secure and resilient to cyber-attacks. If the network is not secure, it could be used to gain access to the system and potentially manipulate or interfere with the automated vehicles.

Hardware Deficiencies

1. Lack of secure hardware: Automated vehicles rely on complex systems of hardware and software, both of which must be secure to ensure the safety of the vehicle and its occupants. The UK does not currently have the same level of secure hardware in place as other countries, and this could easily become a target for cyber-attacks.
2. Outdated technology: The UK's current infrastructure for automated vehicles is outdated and does not have the necessary security measures in place to protect against cyber threats. This could put the safety of the vehicle and its passengers at risk.

Software Deficiencies

1. Lack of secure software: Automated vehicles rely on complex systems of software, both of which must be secure to ensure the safety of the vehicle and its occupants. The UK does not currently have the same level of secure software in place as other countries, and this could easily become a target for cyber-attacks.
2. Vulnerability to malware: Automated vehicles are vulnerable to malware attacks, which could compromise the safety of the vehicle and its occupants. The UK does not currently have the same level of secure software in place as other countries, and this could easily become a target for cyber-attacks.
3. Lack of privacy protection: Automated vehicles collect and store a large amount of data, which must be securely stored and protected against potential cyber threats. The UK does not currently have the necessary privacy protections in place, which could put the safety of the vehicle and its occupants at risk.
4. Unsecured communication networks: Automated vehicles rely on secure communication networks to

e-ISSN: 2583-3472

ensure the safety of the vehicle and its occupants. The UK does not currently have the same level of secure communications networks in place as other countries, and this could easily become a target for cyber-attacks.

Privacy:

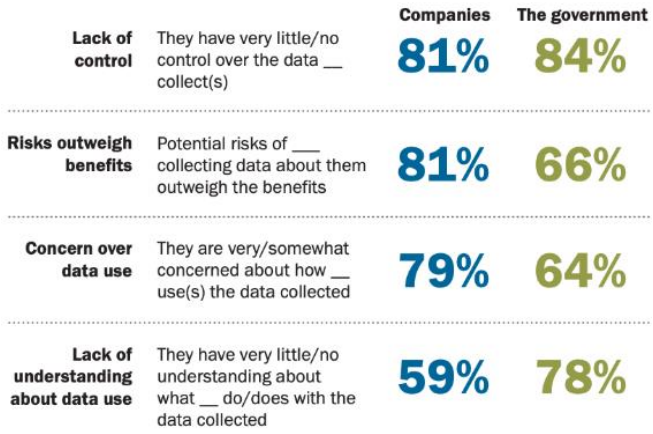

Figure 2 : Privacy Concern Aspect
(Source : He et al. 2020)

Unregulated Data Collection

Unregulated data collection from connected vehicles: Automated vehicles can collect a vast amount of data as they are connected to each other and the internet. This data can be used for various purposes, including tracking individual drivers, their behavior, and even their locations. This can raise serious privacy concerns, as the data collected is not regulated or controlled by any authority.Security threats from hackers: Automated vehicles are connected to the internet, which makes them vulnerable to cyber-attacks from hackers (Liu et al. 2020). These hackers could gain access to the vehicle systems and compromise the safety of the driver and other road users.Security breaches in communication networks: Automated vehicles communicate with each other and infrastructure equipment through wireless networks. These networks can be vulnerable to security breaches, as hackers could gain access to the network and disrupt the communication between vehicles and infrastructure.

This could lead to traffic accidents and other safety issues.Lack of secure authentication and authorization systems: Automated vehicles need secure authentication and authorization systems to prevent unauthorized access to the vehicle systems. If these systems are not secure, it could lead to malicious access to the vehicle systems and compromise the safety of the driver and other road users.Insufficient security measures in vehicle-to-vehicle communication: Vehicle-to-vehicle communication is an important component of automated vehicles. However, the security measures in this communication need to be improved to prevent malicious access to the vehicle systems.

Automated vehicles generate vast amounts of data when in operation. This data includes audio, video, location and other data that can be used to understand the driver's behavior and the vehicle's environment. The UK's lack of regulation around how these data sets can be used and stored can lead to privacy and security concerns. Without proper regulation, companies may collect and store data from drivers without their knowledge, leading to potential misuse of the data. Additionally, the vehicle's automated systems can be vulnerable to hacking, allowing malicious actors to potentially control the vehicle remotely.

Insufficient Security Measures

Automated vehicles are reliant on software and hardware systems to properly function. If these systems are not properly secured, malicious actors can exploit these vulnerabilities to gain access to the vehicle's data and control systems. Additionally, a lack of security measures can also lead to potential data theft from the vehicle's systems.

Data Privacy

The data generated by automated vehicles can contain personal information about the driver, such as location data, audio, video and other data. Without proper regulation, companies may collect and store this data without the driver's knowledge or consent. This can lead to the potential misuse of the data, including potential violations of the driver's privacy.

Lack of Standards

The UK currently lacks standards and regulations regarding automated vehicles. This can lead to a lack of consistency in the safety and security of the vehicles, as well as the data they generate. Without proper standards, it can be difficult to ensure that automated vehicles are properly designed and implemented.

Inadequate Safety Protocols

Automated vehicles can present a number of safety issues, such as the potential for collisions and other hazardous situations. Without proper protocols in place, these risks can be difficult to mitigate. Additionally, automated vehicles can be vulnerable to malicious actors, who can exploit any vulnerabilities in the system to potentially cause harm.

Location Tracking

The implementation of automated vehicles in the UK could pose several cybersecurity risks. One of the key issues associated with automated vehicles is the potential for location tracking. Automated vehicles are equipped with GPS systems and other sensors that allow them to track their location. This data could be used to build a profile of the vehicle's movements, potentially revealing sensitive information about the vehicle's occupants. Automated vehicles would also be able to store data regarding the driving habits of their occupants, including the frequency and duration of trips. This data could be used to identify patterns in the behavior of the occupants and could be used to identify their location when the vehicle is not in use. This data could then be accessed by unauthorized individuals, potentially leading to privacy breaches.

Automated vehicles are becoming increasingly popular in

e-ISSN: 2583-3472

the UK, which is leading to a number of cybersecurity issues related to their implementation. Location tracking is one of the main issues posed by automated vehicles. The technology used in automated vehicles enables them to track their exact location and this data can be used to identify the driver's personal information, such as their residential address, commute times and routes, and their daily activities (Maple et al. 2019). This data can be used by third parties for marketing and other purposes, raising concerns about privacy and data protection. Additionally, if this data is not properly secured, it could be accessed by malicious actors, putting the driver's safety at risk.

Another issue is the potential for hackers to gain access to the vehicle's operating system. Automated vehicles rely on complex computer systems to control their functions and if these systems are not properly secured, hackers could gain access and take control of the vehicle. This could have serious implications for both the driver and other road users and could lead to catastrophic accidents.

Finally, there is the threat of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications being intercepted by malicious actors. Automated vehicles rely on V2V and V2I communications to interact with other vehicles and infrastructure, and if these communications are not adequately protected, they could be intercepted and used to access the vehicle's systems. This could lead to the data being stolen or manipulated, potentially leading to dangerous situations on the roads.

Unauthorized Surveillance

One of the key cybersecurity issues associated with implementing automated vehicles in the UK is unauthorized surveillance. Automated vehicles use sensor data to make decisions, and these sensors may be vulnerable to hacking and unauthorized surveillance. For example, hackers may be able to intercept the data being sent to and from the vehicle, thus gaining access to sensitive information such as the vehicle's location, speed, and direction. Additionally, malicious actors may be able to gain access to the vehicle's onboard systems, allowing them to control the vehicle without the driver's knowledge. This could potentially create a situation in which an attacker could gain control of a vehicle and cause it to crash, potentially resulting in injury or death. The UK government must take steps to ensure that the data sent to and from automated vehicles is secure and that unauthorized surveillance is not possible.

The implementation of automated vehicles in the UK introduces the potential for unauthorized surveillance by malicious actors. Automated vehicles are equipped with sensors and cameras that can collect data about their environment and the people who interact with them. This data can be accessed by unauthorized third parties, potentially leading to privacy violations, identity theft, and other forms of cybercrime. Additionally, automated vehicles may also be vulnerable to attack from malicious actors, who could potentially manipulate their sensors and cameras to gain access to sensitive data (Chen et al. 2020). This could lead to a loss of control over the vehicle, or the manipulation of its systems to cause harm or disruption. Finally, automated vehicles may be vulnerable to malware attacks, which could allow malicious actors to take control of the vehicle and use it for malicious purposes.

Automated vehicles, while offering a secure, efficient, and convenient form of transportation, may also be vulnerable to unauthorized surveillance. Automated vehicles are equipped with a variety of sensors and cameras to monitor their environment, which can be used to monitor the behaviour of drivers and passengers, as well as the surrounding area. As such, automated vehicles in the UK may be at risk of being hacked and the data collected used for malicious purposes.

Data Breaches

Data breaches are a major concern with any technology that stores or transmits data. Autonomous vehicles can store and transmit data such as location and driving data, which could be vulnerable to malicious actors. This data could be used to target vulnerable individuals, manipulate data, or potentially steal identities. The UK government must take measures to ensure that data stored in and transmitted by automated vehicles remains secure and private.

Privacy Concerns

Automated vehicles are equipped with a variety of sensors and cameras, which can collect vast amounts of data about the environment, driver, and passengers. This data can be used to create detailed profiles of individuals, which could be used for marketing purposes or to target vulnerable individuals. The UK government must ensure that data collected by automated vehicles is kept secure and only used for legitimate purposes.

CONCLUSION

The implementation of automated vehicles in the UK presents a wide range of cybersecurity issues that must be addressed. These include potential cyber-attacks on the vehicles themselves, as well as the networks and systems that support them. Additionally, there is the potential for data privacy and security breaches, as well as the risk of malicious actors using the vehicles for illegal activities. In order to ensure the successful implementation of automated vehicles in the UK, it is essential that these cybersecurity issues are addressed and managed appropriately. This requires the development of comprehensive security measures, such as encryption, authentication, access control, and monitoring, as well as policies and procedures that ensure the security of data and systems. With the right measures in place, automated vehicles in the UK can be a safe and secure form of transportation.

REFERENCES

[1] Akowuah, F. and Kong, F., 2021, April. Physical invariant based attack detection for autonomous vehicles: Survey, vision, and challenges. In *2021 Fourth International Conference on Connected and Autonomous Driving (MetroCAD)* (pp. 31-40). IEEE.

e-ISSN: 2583-3472

[2] Channon, M. and Marson, J., 2021. THE liability for cybersecurity breaches of connected and autonomous vehicles. *Computer Law & Security Review*, *43*, p.105628.

[3] Chen, S.Y., Kuo, H.Y. and Lee, C., 2020. Preparing society for automated vehicles: Perceptions of the importance and urgency of emerging issues of governance, regulations, and wider impacts. *Sustainability*, *12*(19), p.7844.

[4] Dixit, P. and Silakari, S., 2021. Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, *39*, p.100317.

[5] Eziama, E., Awin, F., Ahmed, S., Marina Santos-Jaimes, L., Pelumi, A. and Corral-De-Witt, D., 2020. Detection and identification of malicious cyber-attacks in connected and automated vehicles' real-time sensors. *Applied Sciences*, *10*(21), p.7833.

[6] Faisal, A., Kamruzzaman, M., Yigitcanlar, T. and Currie, G., 2019. Understanding autonomous vehicles. *Journal of transport and land use*, *12*(1), pp.45-72.

[7] Gandia, R.M., Antonialli, F., Cavazza, B.H., Neto, A.M., Lima, D.A.D., Sugano, J.Y., Nicolai, I. and Zambalde, A.L., 2019. Autonomous vehicles: scientometric and bibliometric review. *Transport reviews*, *39*(1), pp.9-28.

[8] He, Q., Meng, X. and Qu, R., 2020. Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles. *Journal of advanced transportation*, *2020*.

[9] He, Q., Meng, X., Qu, R. and Xi, R., 2020. Machine learning-based detection for cyber security attacks on connected and autonomous vehicles. *Mathematics*, *8*(8), p.1311.

[10] Linkov, V., Zámečník, P., Havlíčková, D. and Pai, C.W., 2019. Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in psychology*, *10*, p.995.

[11] Liu, N., 2021. *Exploring Public Acceptance of Connected and Autonomous Vehicles with a Focus on Cyber Security and Privacy Risks* (Doctoral dissertation, University of Huddersfield).

[12] Liu, N., Nikitas, A. and Parkinson, S., 2020. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation research part F: traffic psychology and behaviour*, *75*, pp.66-86.

[13] Maple, C., Bradbury, M., Le, A.T. and Ghirardello, K., 2019. A connected and autonomous vehicle reference architecture for attack surface analysis. *Applied Sciences*, *9*(23), p.5101.

[14] Mladenović, M., Stead, D., Milakis, D., Pangbourne, K. and Givoni, M., 2020. Sociotechnical imaginaries of connected and automated vehicle technology: Comparative analysis of governance cultures in Finland, Germany, and the UK.

[15] Mladenović, M.N., Stead, D., Milakis, D., Pangbourne, K. and Givoni, M., 2020. Governance cultures and sociotechnical imaginaries of self-driving vehicle technology: Comparative analysis of Finland, UK and Germany. In *Advances in transport policy and planning* (Vol. 5, pp. 235-262). Academic Press.

[16] Nikitas, A., Njoya, E.T. and Dani, S., 2019. Examining the myths of connected and autonomous vehicles: analysing the pathway to a driverless mobility paradigm. *International Journal of Automotive Technology and Management*, *19*(1/2), pp.10-10.

[17] Seuwou, P., Banissi, E. and Ubakanma, G., 2020. The future of mobility with connected and autonomous vehicles in smart cities. In *Digital twin technologies and smart cities* (pp. 37-52). Springer, Cham.

[18] Taeihagh, A. and Lim, H.S.M., 2019. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport reviews*, *39*(1), pp.103-128.

[19] Tan, S.Y. and Taeihagh, A., 2021. Adaptive governance of autonomous vehicles: Accelerating the adoption of disruptive technologies in Singapore. *Government Information Quarterly*, *38*(2), p.101546.