ENDPOINT (EDP) SECURITY - SECURING VEHICLE AND DRIVER DATA IN A SMART HIGHWAY

1. Introduction

In today's digital age, technologies have been at the forefront of enabling businesses and individuals conduct businesses effectively. Technologies have provided the means for getting information firsthand at your fingertip. The integration of advanced technologies into transportation systems has transformed the way vehicles communicate with one another and the various technologies used for transferring information between systems. The fundamental technological infrastructure to support smart highway systems is Internet of Things (IoT). IoT systems are composed of both digital and physical elements, like interconnected objects and devices, distributed across the network and stretching from the Edge to the Cloud [1]. The concept of a smart highway system, where vehicles and traffic infrastructure are interconnected through Internet of Things (IoT) and other digital technologies, promises significant improvements in traffic management, road safety, and overall transportation efficiency. However, this connected environment also introduces new cybersecurity challenges, particularly regarding the protection of sensitive data transmitted between vehicles, drivers, and roadside infrastructure [2][3].

EndPoint (EDP) security is an essential aspect of ensuring the privacy, integrity, and availability of data in smart highway systems. The term "EndPoint" refers to any device or node within the network, including vehicles, sensors, road signs, and communication hubs, which can be potential targets for cyberattacks. As the volume of data exchanged grows, so does the risk of unauthorized access, data breaches, and malicious manipulation that can compromise not only individual vehicles but also the entire smart highway ecosystem. Ensuring the security of both vehicle data (e.g., location, speed, and driving patterns) and driver information (e.g., personal details, preferences, and biometrics) is crucial for maintaining public trust and the smooth functioning of these advanced systems.

This research focuses on exploring innovative solutions to safeguard the vehicle and driver data within smart highway systems through robust EndPoint security mechanisms. It aims to address the challenges posed by the dynamic and interconnected nature of these systems, while proposing methods for protecting against data vulnerabilities, ensuring privacy, and mitigating the risks of cyberattacks [4][5]. By examining the current state of endpoint security in vehicular networks and offering potential improvements, this study aims to contribute to the creation of more secure, resilient, and trustworthy smart transportation environments. The research of endpoint security in smart highway systems is important to industry and academia because it introduces numerous benefits that can be leveraged to ensure the continuous improvement of already existing cybersecurity controls in discussion.

a) **Improvement to risk management practices:** Endpoint security controls play a pivotal role in achieving compliance objectives by enforcing the principle of least privilege, ensuring availability of audit trails, and ensuring continuous data confidentiality and integrity. This research fosters solutions that align with specific regulatory requisites such as GDPR, PCI DSS, FedRAMP, ISO 27001, and ISO/SAE 21434 which can assist organizations reduce the risk of cyberattacks.
b) **Improved and secure environment:** Businesses are embracing emerging technologies like cloud computing, edge computing, Artificial Intelligence. The security of various endpoint systems that process and store vehicle and driver details grow increasingly complex, with challenges spanning identity management. This research will delve into addressing these challenges by devising various cybersecurity controls like Identify and Access Management, Vulnerability Management, data integrity controls and protocols optimized for cloud-native solutions that facilitate seamless integration, interoperability, and security across on-premises and cloud-based services.
c) **Improved user access management:** In today's dynamic business environment, the security of various endpoint systems ensures the integrity and confidentiality of systems are maintained. This research looks at the adoption of controls like Single Sign-On (SSO) solutions, and role-based access control (RBAC) models to simplify protection and access to endpoints while optimizing resource utilization.
d) **Enhanced Network Integrity:** Endpoints systems often serve as entry points for hackers targeting the broader network. By implementing robust endpoint security, organizations can prevent attackers from exploiting vulnerable devices to infiltrate and compromise internal networks, thereby maintaining the integrity of driver and vehicle information as well as continuously maintaining the confidentiality of critical business infrastructure.

The importance of continuous security of smart highway systems cannot be overemphasized. Security of smart highway systems ensures continued protection of data at all levels through the implementation of data security controls and access control mechanisms. Secondly, public trust among transportation companies, government agencies and other stakeholders is won, which is demonstrated by continuous commitment to develop and implement cybersecurity frameworks and controls which will always ensure the continuous protection of data.

2. Problem statement

The advancement in technology, faster internet speed and emergence of modern technologies has increased the risks of compromise to vehicle and driver data which are processed and stored. Without an effective information security strategy, organizations that process and store these data are at risk of having their systems and data compromised leading to unauthorized access to data, data breaches, compliance violations. Therefore, it is important that a cohesive cybersecurity strategy is developed and implemented to reduce the risk of compromise to systems processing and storing vehicle and driver information.

3. Nature and Significance of the Problem

As smart highway systems continue to evolve, they are becoming increasingly reliant on interconnected technologies that enable vehicles, infrastructure, and drivers to communicate seamlessly. This interconnectivity offers significant benefits in terms of improved traffic management, enhanced safety, and optimized vehicle performance. However, these critical systems are exposed to critical vulnerabilities, particularly in the realm of data security. Vehicle and driver data such as location, speed, and personal information are transmitted through multiple endpoints which can be susceptible to interception leading to data compromise. Unauthorized access to this data can lead to profound consequences, including identity theft, privacy violations, traffic disruptions, and even potential accidents caused by malicious interference with vehicle systems. Without proper security measures in place, the entire ecosystem of a smart highway system is at risk.

This study aims to address these pressing security challenges by focusing on endpoint (EDP) security within smart highway systems. By examining current vulnerabilities and potential risks associated with vehicle and driver data, the study will provide valuable insights into effective security solutions. The study will help identify gaps in existing security protocols and propose comprehensive strategies to safeguard critical endpoints in the system. The findings will contribute to developing advanced security frameworks that enhance data protection, prevent unauthorized access, and mitigate the risks of cyberattacks. This study will be instrumental in guiding industry stakeholders—such as vehicle manufacturers, infrastructure developers, and policymakers—in implementing best practices for endpoint security. The study will play a crucial role in ensuring that the future of smart highways is both secure and resilient, enabling safer, more efficient transportation systems for all users [6].

Below are the theories this study influences:

a) **Privacy theory:** Theories relating to data privacy and rights emphasize the importance of ensuring the continuous protection of driver and vehicle data in a smart highway system. Ensuring the data privacy and integrity of the driver information will prevent malicious practices like impersonation, identify theft, and unauthorized access to sensitive information like vehicle identification number, chassis number etc. This is crucial in preventing misuse of sensitive information.
b) **Risk Management theory:** The focal point of this theory is the ability to identify, assess and mitigate cybersecurity risks that can impact smart highway systems. Implementing an effective risk management process will ensure that events that could lead to the compromise of the smart highway system can be identified and mitigated to ensure continuous confidentiality and integrity of driver and vehicle safety.
c) **Cybersecurity Framework**: The availability of several cybersecurity frameworks like NIST, ISO27001, Digital Operation Regulation Act (DORA), GDPR provides a baseline guideline for managing and ensuring the effective implementation of

information security and privacy controls in a smart highway. Security controls can be mapped into the various cybersecurity frameworks to ensure best practices are followed.

d) **Information Security Theory:** The theory of information security highlights the importance of ensuring that confidentiality, integrity, and availability of information systems is always maintained in a smart highway system. Ensuring the continuous security of vehicle and driver data supports the basic objectives of information which is protecting data always.

4. Objectives of the Study

The objectives of the study of ensuring the security of driver and vehicle information on endpoint in smart highway are as follows:

a) Determine how vulnerabilities in smart highway systems can be exploited to compromise driver and vehicle data.
b) To explore the impact of vulnerabilities in smart highway systems. Vulnerabilities or weaknesses in endpoint systems pose tremendous challenges to the safety of driver and vehicle data in a digitized world.
c) To assess the impact of data breaches on endpoint systems: The impact of inadequate security controls in a smart highway system cannot be oversimplified. Compromise of endpoint systems will lead to breach of data privacy, reputational damage, and financial loss.
d) Examine how access control mechanisms can maintain confidentiality of vehicle and driver data.

5. Hypotheses

a) Organizations with robust endpoint security strategies and controls experience lesser security breaches and unauthorized access to data.
b) Implementing robust network security and access control can lead to increased data security.
c) Centralized Identity Access Management (IAM) systems are more efficient in managing user access to systems.
d) A comprehensive vulnerability management program identifies application and system weaknesses early leading to it being resolved before hackers take exploit it.
e) The use of Multifactor Authentication (MFA) within smart highway systems enhances user access controls.
f) Adherence to cybersecurity standards and frameworks will ensure implementation and monitoring of cybersecurity controls.
g) Organizations that invest in comprehensive cybersecurity training and awareness programs have higher incident identification.
h) Effective monitoring of cybersecurity controls ensures cyberattacks can be detected sooner instead of later.

6. **Definition of Terms**
    a) **Identify Access Management:** cybersecurity practice that manages how users access digital resources within an organization, ensuring only authorized individuals have the appropriate level of access to specific information and systems.
    b) **Internet of Things:** a network of physical objects that can connect and exchange data with other devices and systems over the internet.
    c) **Cyber-Physical:** Mechanisms controlled and monitored by computer algorithms, tightly integrated with the internet and its users. In cyber-physical systems, physical and software components are deeply intertwined, able to operate on different spatial and temporal scales, exhibit multiple and distinct behavioral modalities, and interact with each other in ways that change with context.
    d) **Cloud Computing:** the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
    e) **Smart highway:** a highway that uses electronic technologies to improve the operation of vehicles, traffic, and road conditions.
    f) **Endpoint systems:** physical devices that connect to and exchange information with a computer network.
    g) **Authentication**: the process of determining whether someone or something is who or what they say they are
    h) **Authorization:** The process of allowing users to gain access to systems based on their access rights.
    i) **Cyberattack:** an attempt by actors to damage or destroy a computer network or system.

7. Literature Review

The intersection of endpoint security and smart highway systems is an emerging area of study, driven by the rapid adoption of connected and autonomous vehicle technologies. As vehicles, infrastructure, and drivers exchange large volumes of data, the need for robust security mechanisms has become a critical concern [7]. This is because a compromise of these systems could lead to tremendous impact on the organizations processing and storing this information. Cyberattackers always device new ways to circumvent cyber controls to gain access to sensitive and confidential information [8][9]. This literature review explores the key concepts of endpoint security on smart highway systems, and their associated cybersecurity challenges. Additionally, the study will highlight the current gaps that attackers can leverage on to gain unrestricted access to sensitive data.

Vehicles in smart highway systems generate a vast amount of data, including location, speed, driving behavior, and other sensor data. Driver information such as personal preferences, biometrics, financial and payment details are also frequently transmitted. According to recent research, data is sensitive, and its protection is

paramount for maintaining privacy and security [8][9][10]. The increasing use of cloud computing, in-vehicle networks, and communication channels further amplifies the exposure of data to cyber threats [11]. Studies have highlighted how vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications could be exploited if endpoints are not adequately secured, leading to potential data breaches and unauthorized access [12]. Endpoint security refers to the protection of devices that interact with the network, such as vehicles, sensors, roadside units, and communication gateways. These endpoints are potential targets for cyberattacks, which can compromise both the device and the broader system [12][13][14]. Existing research on endpoint security in vehicular networks, shows that many of these endpoints lack sufficient protection against attacks like man-in-the-middle, spoofing, and denial-of-service (DoS) [15]. As endpoints function as entry points to larger systems, their compromise can lead to cascading failures across the entire transportation network. Additionally, endpoint devices in smart highway ecosystems, especially autonomous vehicles, must be protected from both external and internal threats [14][15]. External threats include malicious actors attempting to hijack or manipulate vehicle control systems, while insider threats could involve unauthorized or disgruntled employees who are exploiting vulnerabilities within the vehicle's onboard systems.

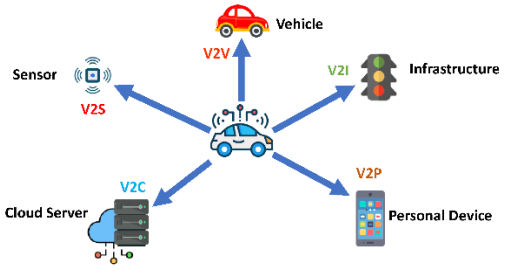

Figure 1: Architectural representation of a Vehicle-to-Vehicle in smart highway system.

Numerous security protocols and frameworks have been proposed to protect the data exchanged within vehicular networks. Cryptography, for instance, is commonly used to encrypt communication between endpoints, ensuring that data is secure before and during transmission. Recent studies have proposed the use of public key infrastructure (PKI) for securing vehicle-to-infrastructure communications [16][17][18]. The implementation of advanced encryption techniques can prevent interception and ensure data privacy [19][20][21]. Privacy is a major concern when dealing with vehicle and driver data, as much of the information exchanged through smart highway systems is personal and sensitive. Regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States aim to protect individuals' data privacy rights, but challenges remain in enforcement within dynamic, interconnected environments like smart highways. There has been the emphasis on the need for privacy-preserving techniques, such as anonymization or pseudonymization of driver data, to comply with privacy regulations and safeguard user identities from being exposed or misused. In the context of endpoint security, ensuring compliance with these regulations requires the implementation of stringent access controls, data encryption,

and audit mechanisms [20]. A comprehensive approach to endpoint security must consider both technical safeguards and legal frameworks to ensure that smart highway systems are secure and compliant with privacy laws [21].

CHALLENGES TO ENDPOINT SECURITY

The implementation of technology is to assist in helping businesses to operate efficiently. However, endpoints do pose security challenges to the environment they are being operated on. These include:

i. **Limited Computational Power:** Many endpoints in smart highway systems, such as sensors and roadside devices, are constrained by limited computational resources. These devices often lack the processing power to run complex security algorithms or real-time threat detection systems. This limitation forces the use of lightweight security protocols, which may not provide sufficient protection against advanced cyberattacks, thereby leading to compromise of data integrity and system availability.

ii. **Existence of vulnerabilities:** Endpoints are often targeted in cyberattacks, as they are the entry points into the broader network. Attacks such as Distributed Denial of Service (DDoS), man-in-the-middle (MitM), spoofing, and ransomware can disrupt operations, steal data, or compromise vehicle safety systems. Given the high volume of data exchanged between vehicles and infrastructure, the risk of interception or manipulation of data is a serious concern [22].

iii. **Unsecure Communication Channels:** Endpoints in a smart highway system communicate over wireless networks, which are inherently vulnerable to interception, eavesdropping, or manipulation. Without robust encryption and secure communication protocols, data exchanged between vehicles and infrastructure can be exploited by cybercriminals which undermine the security of the entire system 23][24].

iv. **Lack of Real-Time Security Monitoring:** Real-time monitoring of endpoint security across a large and dynamic smart highway system is difficult to implement. As vehicles and infrastructure move and interact with one another, vulnerabilities can emerge unpredictably. Real-time threat detection systems and centralized security monitoring frameworks are needed to identify and respond to security incidents promptly, but their implementation can be resource-intensive and challenging to manage at scale [24].

v. **Supply Chain Security:** Many of the components that make up smart highway endpoints such as vehicle hardware, sensors, and communication equipment—are sourced from different suppliers. The security of the entire system depends on the integrity of each component. Vulnerabilities introduced through insecure supply chains can compromise the security of the endpoints leaving the entire smart highway system vulnerable to exploitation [24][25].

SOLUTIONS TO ENDPOINT CHALLENGES

As connected transportation systems evolve new security solutions are continuously being researched. For example, machine learning and artificial intelligence (AI) have been explored for detecting anomaly behavior in vehicular networks. Recent studies have demonstrated how AI-based intrusion detection systems (IDS) can identify potential security threats at endpoints by analyzing traffic patterns and flagging unusual activities [23]. Similarly, adaptive security frameworks that adjust security levels based on the threat landscape are gaining attention in recent research. These solutions promise to improve response times and the effectiveness of endpoint security measures [25][26]. Another promising area of research is the development of lightweight security protocols tailored for resource-constrained devices. As many endpoints such as roadside sensors and embedded vehicle systems have limited computational power, there is a need for security measures that are both effective and efficient.

8. Methodology

Identity and access management security are regarded as the prime element of the entire IT security system that manages digital identities along with user access in the firm. To evaluate the role of IAM, the concern has been laid on making effective utilization of industry standards processes and mechanisms. Below is the schedule of the project.

Project Schedule

Task	**What is involved**	**Time needed**	**Approx. cost**	**Technical expertise needed**	**Gaps in knowledge and skills**
Literature review	Conducting a comprehensive review of existing papers on securing vehicle and driver data in a smart highway.	3 weeks	No cost needed	Research and technical skills to understand the body of knowledge	Lack of knowledge in subjects as well as not being abreast of recent advancement in smart systems.
Instrument construction	Preparing research questions	1-2 weeks	No cost needed	Technical knowledge of how to design surveys	Limited knowledge in the use of technology to create surveys
Data collection	Collect data according to research methodology	3 weeks	Moderate cost since software will be used to create the survey	Inexperience in collecting data for survey.	Lack of technical experience and training in the usage of software for survey.
Data analysis	Perform analysis of data collected using statistical methods	2 weeks	Moderate cost since software will be used in performing the analysis	Statistical analysis method	Difficulties in selecting statistical methods for analysis.

Draft report	Develop draft report on research findings	2 weeks	No cost involved	Writing skills needed to express the research findings in a simple language	Difficulty in articulating research results to conclude and provide recommendations.
Final report	Finalize the draft report in a complete report.	2 – 3 weeks	No monetary cost involved. Only time is needed.	Excellent written skills needed as well as being able to express technical language into simple language.	Difficulty providing conclusions and recommendations from the research study.

Table 1: Project Schedule

i. STUDY DESIGN

The proposed study design is the Case Study design. The case study design seeks to explore and thoroughly uncover the in-depth security measures or mechanisms that will be used to provide adequate security protection of the various endpoint systems. The Case Study design comes with numerous benefits when adopted for research. It harnesses an intersection between theory and practice making it a versatile study design to adopt. It also has the potential of uncovering or generating new findings. Additionally, random sampling methodology was used design for this research because it offers several key advantages, especially when the goal is to ensure that the sample is representative of the broader population. The primary reason for choosing random sampling is its ability to reduce bias since every member of the population has an equal opportunity of being selected. Also, there is a lower likelihood that the sample will favor certain outcomes over others. Lastly, random sampling helps ensure that the selected sample closely reflects the overall population which increases the external validity of the findings. This is particularly important when researchers want to make inferences about a larger group from a smaller sample. Random sampling is straightforward to implement and does not require subjective judgment on the selected population. This can make the process of sampling more transparent.

Data Collection

Research question	Relevant questions in the questionnaire
What are the common vulnerabilities in smart highway systems that could be exploited to access sensitive driver and vehicle data?	a) How familiar are you with the vulnerabilities present in smart highway systems? b) Which of the following vulnerabilities do you consider most critical in smart highway systems? c) Which of the following exploitation methods do you think pose the greatest risk to smart highway systems?
How do successful exploits of smart highway system vulnerabilities affect the integrity and confidentiality of driver and vehicle data?	a) In your opinion, what are the potential consequences of compromised data integrity in smart highway systems? b) How serious do you believe the risks to data confidentiality are in smart highway systems? c) What types of confidential data do you think are most at risk of being compromised?
What are the potential real-world consequences for drivers and vehicles if their data is compromised through vulnerabilities in smart highway systems?	a) How familiar are you with the potential risks associated with data compromise in smart highway systems? b) In your opinion, what are the most significant potential consequences of data compromise for drivers? c) What consequences do you think compromised data could have on vehicle safety? d) How do you think public trust in smart highway systems is affected by data compromise incidents?
What best practices and technologies can be implemented to mitigate the risks associated with vulnerabilities in smart highway systems and protect driver and vehicle data?	a) What strategies do you think are essential for mitigating the consequences of data compromise in smart highway systems? b) How effective do you think current regulations are in protecting driver and vehicle data? c) Which technologies do you believe are crucial for enhancing the security of smart highway systems?

Table 2: Research questions

ii. Tools and Techniques

Conducting research in endpoint security in smart highways involves the use of numerous tools and techniques that can be utilized to gather information. Below is an overview of common tools and techniques the would be used in this research for data gathering.

Surveys and Questionnaires: Surveys and questionnaires will be used for gathering data on endpoint systems in smart highways. Researchers will be able to design surveys to gather quantitative data on topics such as security awareness training, user satisfaction with data privacy methods.

a) **Interviews and Focus Groups:** Interviews of specific focus groups would be used to gather the necessary insights from cybersecurity engineers, security administrators, and system users. These methods enable in-depth exploration of endpoint security controls.

b) **Case Studies:** Case studies involve in-depth analysis of real-world implementations, challenges, and outcomes within specific industries. This technique makes it easy to collect as much information from participants as possible through the use real-life scenarios to which they can easily relate.
c) **Data Analysis Tools:** The use of data analysis tools such as SPSS, R, Python, and qualitative analysis software would make analysis of the survey and interview responses easy to understand and digest.
d) **Simulation and Modeling Techniques:** Simulation techniques will be used to simulate how end-users behave in virtualized environments when faced with cybersecurity incidents. Endpoint security systems will need to be modelled with adequate user access controls, network security controls, data security controls to assess their level of resiliency and scalability.

9. CONCLUSION

To conclude, organizations and business leverage technologies to conduct business. The transport sector has been one industry that has seen the increase adoption of technologies in the form of smart highway systems which provide information to drivers and pedestrians. However, the adoption of these technologies introduces its own cybersecurity risks to the business, drivers, and pedestrians. Lack of comprehensive vulnerability management program for organizations and institutions exposes them to incidence of cyberattack since hackers can easily gain unrestricted access to sensitive resources and information like driver financial information, Personally Identifiable Information (PII), pedestrian information and vehicular details. These acquired information can be used to perpetrate acts such as identity theft, financial fraud etc.

A comprehensive approach is needed to ensure that endpoint security is implemented and always maintained. This will include the use of encryption to ensure confidentiality and integrity of information. Secondly, stringent access control mechanisms such as MFA should be employed to add another layer to security. Additionally, regular awareness training should be conducted for end users of the smart highway systems to adequately equip them on how to conduct themselves whiles using these technologies as well as be on the lookout for abnormal behaviors in the use of the endpoint systems. Implementing controls will build trust, reduce the incidence of legal battles, and preserve the trust stakeholders will have in the use of smart highway systems.

References

1. 1. L. Atzori, A. Iera, G. Morabito The Internet of Things: a survey Comput. Netw., 54 (15) (2010), pp. 2787-2805
2. Arabo, A. (2015). Cyber security challenges within the connected home ecosystem futures. Procedia Computer Science, 61, 227–232. https://doi.org/10.1016/j.procs.2015.09.078
3. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2015). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security, 56*, 1–27. https://doi.org/10.1016/j.cose.2015.01.001
4. Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)* (pp. 1–5). https://doi.org/10.1109/WIRELESSVITAE.2011.5942705
5. ISO/IEC 27001:2013. (2013). *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization (ISO).
6. Tao, Y., Lei, Z., & Ruxiang, P. (2018). Fine-grained big data security method based on zero trust model. In *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 1040–1045). IEEE. https://doi.org/10.1109/ICPADS.2018.00179
7. Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers & Security, 62*, 165–176. https://doi.org/10.1016/j.cose.2016.07.004
8. Honeycutt, D., & Grumman, N. (2013). Developing a framework to improve critical infrastructure cybersecurity.
9. Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In *Artificial Intelligence and Security* (pp. 50–60). Springer. https://doi.org/10.1007/978-3-030-44755-9_5
10. Gilman, E. (2016). *Zero trust networks: Building secure systems in untrusted networks*. O'Reilly Media.
11. Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for Internet of Things (IoT). In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)* (pp. 1–5). https://doi.org/10.1109/WIRELESSVITAE.2011.5942705
12. Biswas, S., Tatchikou, R., & Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communications Magazine, 44*(1), 74–82. https://doi.org/10.1109/MCOM.2006.1609421
13. Department for Transport. (2016). Rail cyber security – Guidance to industry. Technical report, Department for Transport.
14. Raya, M., Papadimitratos, P., & Hubaux, J. P. (2006). Securing vehicular communications. *IEEE Wireless Communications, 13*(5), 8–15. https://doi.org/10.1109/MWC.2006.1707417
15. The Smart Grid Interoperability Panel - Cyber Security Working Group. (2010). *Introduction to NISTIR 7682 – Guidelines for Smart Grid Cyber Security*. Technical report, U.S. Department of Commerce.
16. Xu, Q., Mak, T., Ko, J., & Sengupta, R. (2004). Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks* (pp. 19–28). https://doi.org/10.1145/1026513.1026520

17. Lamba, A. (2015). To classify cyber-security threats in automotive domain using different assessment methodologies. *International Journal for Technological Research in Engineering, 3*(3), 5831–5836.
18. Lamba, A. (2016). S4: A novel & secure method for enforcing privacy in cloud data warehouses. *International Journal for Technological Research in Engineering, 3*(8), 5707–5710.
19. Khairnar, V. D., & Pradhan, S. (2013). Comparative study of simulation for vehicular ad-hoc network. Preprint, *ArXiv:1304.5181*.
20. Pawar, K., Ambhika, C., & Murukesh, C. (2021). IoT hacking: Cyber security point of view. *Asian Journal of Basic Science & Research, 3*(2), 1–9. https://doi.org/10.38177/ajbsr.2021.3201
21. Lamba, A. (2016). S4: A novel & secure method for enforcing privacy in cloud data warehouses. *International Journal for Technological Research in Engineering, 3*(8), 5707–5710.
22. Risk analysis of autonomous vehicles in mixed traffic streams. *Transportation Research Record: Journal of the Transportation Research Board, 2625*, 51–61. https://doi.org/10.3141/2625-06
23. Data security and threat modeling for smart city infrastructure. In *Cyber Security of Smart Cities, Industrial Control Systems and Communications (SSIC) International Conference On* (2015), 1–6.
24. Cyber security challenges in Smart Cities: Safety, security, and privacy. *J. Adv. Res., 5*(4), 491–497.
25. Smart cities: A survey on security concerns. *Int. J. Adv. Comput. Sci. Appl., 7*, 612–625. https://doi.org/10.14569/IJACSA.2016.070481
26. Securing vehicle-to-everything (V2X) communication platforms. *IEEE Transactions on Intelligent Vehicles, 5*, 693–713. https://doi.org/10.1109/TIV.2020.2987430
27. Adversarial attacks and defense in deep reinforcement learning (DRL)-based traffic signal controllers. *IEEE Open Journal of Intelligent Transportation Systems, 2*, 402–416. https://doi.org/10.1109/OJITS.2021.3118972
28. Securing vehicle-to-everything (V2X) communication platforms. *IEEE Transactions on Intelligent Vehicles, 5*, 693–713. https://doi.org/10.1109/TIV.2020.2987430

Word count: 4373

AI tool usage statement: I confirm that I have not used any AI tool for this assignment.