WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security and Privacy issues in the Internet of Vehicles (IoV)

Timothy Murkomen, Leonard Wakoli and Richard Omolo

Jaramogi Oginga Odinga University of Science and Technology

ABSTRACT:

The Internet of Vehicles (IoV) is an emerging technology that is changing the way transportation systems operate as it allows vehicles, infrastructure, and other entities to communicate effectively and work together. It represents a more dynamic and interconnected system that enables seamless vehicular communication. The increase in connectivity with reliance on data exchange brings security and privacy concerns such as the risk of unauthorized access, privacy violations, and data breaches. This paper aims to investigate security and privacy issues in the Internet of Vehicles ecosystem. The paper explores the most common security issues in IoV, including unauthorized access, malicious attacks, and data breaches alongside privacy risks such as location tracking, identity disclosure, and social engineering attacks. The findings of this paper provide valuable insights for developing robust models aimed at enhancing the confidentiality, integrity, availability, authentication and non-repudiation of Internet of Vehicles (IoV) systems. This study proposes research directions, including advanced authentication mechanisms, AI and ML-based attack detection, decentralized blockchain architectures, and real-world testing for IoV security and privacy. It serves as a valuable resource to researchers, policymakers, and decision-makers, contributing to the advancement of Internet of Vehicles security, and paving the way for a safer and more resilient vehicular network.

Index Terms - Internet of Vehicles, Privacy and Security, Vehicular Networks

INTRODUCTION

The Internet of Vehicles (IoV) is transforming vehicular communication as it enables real-time data exchange among vehicles, infrastructure, and other entities [1]. It connects vehicles, infrastructure, and users through advanced networking technologies. This IoV ecosystem enables seamless data exchange to improve traffic management, safety, and user experience. However, the interconnected, dynamic, and open nature of IoV poses security and privacy concerns, necessitating the need for robust mechanisms to protect sensitive data, protecting the confidentiality, integrity, and availability of information hence ensuring trustworthy communication.

Unauthorized access, malicious attacks, and data breaches pose serious risks to the integrity, confidentiality, and availability of information exchanged within this dynamic ecosystem. Addressing these challenges is critical to ensure trust and safety in the IoV environment. Security issues in Internet of Vehicles (IoV), such as denial of service (DoS) attacks, and data manipulation, compromise the integrity and reliability of vehicular networks. These issues disrupt communication, leading to misinformation and potential accidents in the domain. Privacy concerns on the other hand, such as location tracking and identity disclosure, raise questions about user confidentiality. This study is motivated by the need to address these security and privacy concerns.

The study aims to investigate the current state of Internet of Vehicles (IoV) security, exploring potential vulnerabilities, and proposing potential mitigation strategies. The study aims to strengthen the reliability and trustworthiness of vehicular networks. The findings of this study will benefit various stakeholders, including researchers, policymakers, and IoV practitioners. Investing the security and privacy challenges within the Internet of Vehicles (IoV) ecosystem helps to guide the development of strategies to strengthen IoV systems, hence transforming the transportation ecosystem while protecting the rights and privacy of its users.

CONTRIBUTIONS OF THE STUDY

This study provides significant contributions to the field of vehicular communication systems. The key contributions include: 1) IoV security issues: This study identifies prominent security issues within the IoV ecosystem such as Sybil attacks, denial of service (DoS) attacks, eavesdropping, and location spoofing. It explores how these security issues compromise the confidentiality, integrity, and availability (CIA) of vehicular networks hence providing a structured understanding of the threats and vulnerabilities. 2) Privacy Concerns: The study explores privacy issues such as location tracking, identity disclosure, and user consent challenges. These concerns are critical in maintaining user trust in IoV systems. The paper discusses the implications of these issues, including profiling, unauthorized tracking, and social engineering risks. 3) Contribution to Knowledge in Internet of Vehicles: The paper adds to the growing body of knowledge in Internet of Vehicles (IoV) security and privacy. 4) Roadmap for Future Research: The study provides a roadmap for future research; the necessity of developing robust privacy-preserving communication mechanisms for Internet of Vehicles (IoV).

The paper is structured as follows: Section I presents the introduction and the contributions of the study. Section II provides the literature review; the background information; the overview of IoV, communications within IoV and the layers of IoV. Section III presents the security issues in the IoV. Section IV presents the privacy issues in the IoV. Section V presents the discussion and roadmap for future research. Finally, Section VI concludes the paper.

LITERATURE REVIEW

The Internet of Vehicles (IoV) integrates vehicles, infrastructure, and other entities into a connected vehicular network [2]. It builds upon technologies such as the Internet of Things [3], vehicular ad hoc networks (VANETs) [4], and cloud computing to enable seamless communication and data exchange. IoV systems facilitate intelligent transportation by improving road safety, reducing congestion, and providing real-time information to drivers. For example, IoV applications include traffic management, collision avoidance systems, autonomous driving, and personalized infotainment services. Despite the promising potential, IoV systems face security and privacy challenges.

The interconnected and dynamic nature of IoV coupled with the voluminous data that is generated and exchanged increases security, exposing networks to risks such as unauthorized access, data breaches, and malicious attacks. Security issues, including Sybil attacks, denial of service (DoS) attacks, and data manipulation, compromise the reliability and functionality of vehicular communication. Privacy concerns arise from the continuous exchange of sensitive information, such as vehicle locations and user identities, making IoV networks vulnerable to tracking, profiling, and unauthorized disclosure.

Many scholars have developed various security and privacy preservation mechanisms in IoV to address the privacy and security concerns in the Internet of vehicles ecosystem. Cryptographic techniques, authentication protocols, and access control mechanisms are commonly used to protect data confidentiality, integrity, and availability (CIA). Privacy-preserving mechanisms such as location obfuscation and data minimization, aim to safeguard user information without compromising system functionality. However, the interconnected, dynamic and open nature of IoV systems creates additional complexities, requiring more robust and innovative solutions. This research builds upon existing studies by focusing on the security and privacy issues specific to IoV ecosystems. It aims to investigate the privacy and security issues within the IoV ecosystem.

OVERVIEW OF INTERNET OF VEHICLES

The Internet of Vehicles (IoV) is a comprehensive ecosystem that combines IoT technologies and intelligent transportation systems [5]. IoV expands its structure and uses of the Vehicular Ad hoc Networks (VANETs) to provide a wide variety of services [6], such as the smart traffic control, self-driving cars, improved driving safety, accurate navigation, fast response to accidents, effective vehicle management, and convenient features like remote door unlocking and vehicle theft recovery. IoV also offers entertainment options such as infotainment services [7]. The combination of IoT and intelligent transportation systems in IoV opens up fascinating possibilities for advanced vehicle communication [8]. Internet of Vehicles (IoV) involves a wide variety of participants, including vehicles, drivers, passengers as users, sensors (e.g., on traffic lights), and On-Board Units (OBUs) that are installed on the vehicles to provide intelligent capabilities [9].

A Central Authority (CA) is responsible for network access and maintenance, while cloud servers handle communications and storage. In addition, Roadside Units (RSUs) are strategically placed along the roads to facilitate the communication between vehicles and infrastructures. According to [10], the mentioned participants usually engage in multiple communications, which includes the Vehicle-to-Vehicle (V2V), which refers to direct communication between vehicles. It allows vehicles to share information such as speed, location, and direction with each other.

Vehicle-to-Road (V2R) which involves communication between vehicles and the road infrastructure, such as traffic signs, signals, and road conditions. Vehicle-to-Human (V2H) which focuses on interactions between vehicles and pedestrians or cyclists. Vehicles-to-Infrastructure (V2I) is similar to V2R, it involves vehicles interacting with various infrastructure elements like traffic lights and parking systems. Vehicle-to-Devices (V2D) refers to the communication between vehicles and various devices, such as smartphones. It facilitates activities such as remote vehicle control, and infotainment services.

Vehicle-to-Sensor (V2S) that focuses on the communication between vehicles and sensors installed on the vehicle itself and or its environment, for example the road sensors. The sensors help in collecting data on vehicle performance, environmental conditions. These interactions collectively form a social network of intelligent objects. The objects exchange traffic information through the Safety Beacon Messages (SBM) [11], [12]. Fig. 1 shows the visual representation of IoV Communications.

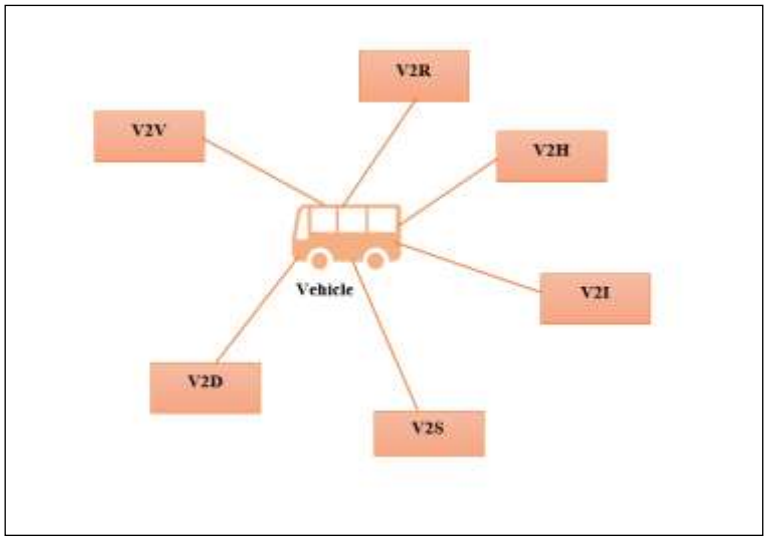

Fig.1. Sample Visual Representation of IoV Communications (Researcher, 2024)

Layers OF INTERNET OF VEHICLES

In Internet of Vehicles (IoV) architecture, there are four layers and each layer with its own unique capability. The first layer is the Environment Sensing and Control Layer that gathers information from the sensors in the environment. The second layer is the Network Access and Transport Layer that handles communication management. The third layer is the Coordinative Computing layer and is responsible for system management. Lastly, the Application Layer stores and analyzes data and provides various services which includes open and closed services to meet different needs. This centralized system relies on Trusted Central Authorities (CA) to ensure security and integrity [13]. Fig.2 below shows the components of IoV Architecture.

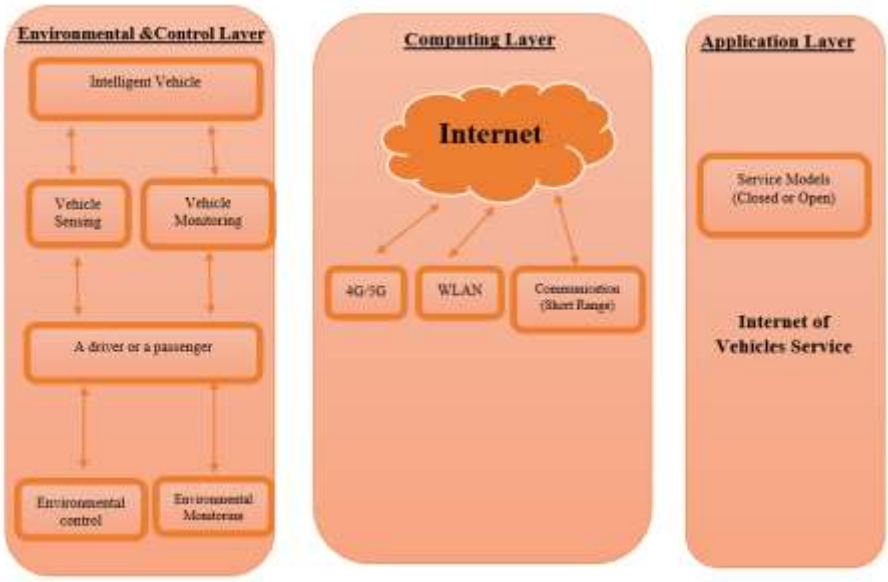

Fig.2. The components of IoV Architecture (Researcher, 2024)

SECURITY AND PRIVACY IN IOV

According to [14] and [15], there exist privacy and security concerns in the vehicular communications due to its dynamic nature. A key issue is the vulnerability to malicious attacks which include denial of service attacks, data manipulation, and unauthorized entry which affect the core principles of information security which includes the integrity of the data exchanged by various parties in the Internet of Vehicles ecosystem. Location information and driving patterns raise privacy issues since it can be exploited through tracking or user profiling.

There are security and privacy requirements for vehicular communications that help strengthen the confidentiality, integrity and availability of data. Authentication and non-repudiation in vehicular networks help to ensure that only authorized entities can participate in communication and helps establish accountability and trust in communications respectively. Message integrity in internet of Vehicles (IoV) means that the content of the data exchanged between vehicles, infrastructure and other entities cannot be altered or manipulated.

Data confidentiality involves protecting the content of the data exchanged between the vehicular infrastructure from unauthorized access. Access control controls and monitors who, what and when a subject can perform actions within the system. According to [16], attacks are classified and grouped in CIA Triad framework. Protecting the CIA triad in vehicular networks necessitates the implementation of enhanced encryption mechanisms for integrity, confidentiality and authentication protocols.

Fig.3: CIA Triad attacks, (Researcher, 2024)

Authentication helps in verifying the identity of a vehicular entity, while the access rights are determined by the authorization. The biggest challenge is verifying the authentication of vehicles to ensure they are genuine and the vehicular communication are safeguarded against unauthorized participants since IoV ecosystem are open and have dynamic nature. The major challenge is their open and dynamic nature which makes authentication impossible while unauthorized people could compromise network integrity [17].

Vehicular networks are dynamic in nature with vehicles that enter and leave the network frequently. Sybil attacks compromise the integrity and reliability of the network by creating sybil nodes (malicious entities) that impersonate the vehicular entities and disrupt communications, spread false information or even manipulate the network [18]. Denial of Service attacks involves overwhelming network resources such as the communication channels hence preventing legitimate vehicles and entities from accessing the very essential services [19], [20]. This attack disrupts vehicular communication hence affecting the network functionality.

According to [21], a form of attack known as communication jamming involves transmitting interference signals with the aim of disrupting the wireless communication channels hence causing congestion and blocking legitimate messages. Resource exhaustion attacks aim to exhaust the network resources such as the bandwidth, the processing power, the memory, by injecting the network with voluminous and malicious traffic [22]. Location spoofing involves manipulating the location related information which leads to false positioning of data that is disseminated in the network. The false information disseminated can lead to incorrect decisions by the entities in the ecosystem and results to accidents or traffic flow disruptions [23].

Eavesdropping attacks intercept sensitive information that is exchanged between the vehicles and infrastructure [24]. The aim of eavesdropping is to gain access to the information such as the location data, communication patterns and personally identifiable information (PII). Eavesdropping compromises the confidentiality of sensitive information. Table 1 below summarizes the security challenges in vehicular networks.

Table 1: Security Challenges in Vehicular Networks (Researcher, 2024)

Security Issue	Explanation	Effects
Authentication and Authorization	Exploiting vulnerabilities in the verification end approval mechanisms in systems.	Disrupts the communication, compromise safety and leads to lack of privacy.
Sybil attack	Creation of multiple fake identities to flood a network, hence disrupting vehicular communication.	Impersonation of vehicular entities, leading to misinformation and the disruption of network services.
Denial of Service attack	Overloading the vehicular network	Disruption of communications
Location Spoofing	Attacker providing false location information to other vehicles or other vehicular infrastructure, and creating a deceptive representation of its position.	Traffic congestion, collision risks, and misleading navigation of vehicles.
Eavesdropping	Refers to unauthorized interception of communication	Leads to unauthorized access to sensitive information

PRIVACY ISSUES IN IOV ECOSYSTEM

Due to the continuous exchange of location data and other sensitive information among various entities, leads to privacy issues in the IoV ecosystem. Safeguarding individual privacy is very crucial as it prevents potential misuse of personal data [25], [26]. Location privacy involves the location related privacy issues that lead to the tracking of individual vehicles, or profiling, and leads to compromising the privacy of the vehicle. Malicious actors can exploit the location data to track and monitor the movement of specific vehicles hence raising privacy concerns to the passengers and the driver [27].

Identity disclosure involves unauthorized exposure of the entity's real identity. Data minimization involves collecting only the minimum amount of data that is necessary for a given purpose. In Internet of Vehicles (IoV) ecosystem that is dynamic in nature and data is continuously processed, data minimization helps address privacy concerns [28]. In terms of user consent and control, users should be given the authority to control their personal data and make informed decisions about its usage.

The dynamic nature of Internet of Vehicles (IoV) makes it challenging in obtaining and maintaining user consent. Social engineering attacks involves attackers deceiving individuals into giving out confidential and sensitive information, providing access to systems and leading to activities that may compromise security. Social engineering relies on human psychology, and entities in the IoV ecosystem are primary susceptible to technical challenges, and social engineering can be used to manipulate users to compromise the security of the network [29]. Table 2 summarizes the privacy issues in IoV ecosystem.

Table 2: Privacy issues in IoV ecosystem (Researcher, 2024)

Privacy Issue	Explanation	Effects
Location privacy	Location privacy refers to the manipulation of location information	Compromises traffic flow, and misguides other entities leading to poor coordination
Identity Disclosure	Identity disclosure refers to the exposure of entity's real identity	Leads to tracking and user profiling and misuse of personal information
User consent and control	User consent and control as a privacy issue refers to lack of mechanisms control the data and providing consent	The users may be unable to manage the data sharing leading to exposure of personal information unknowingly
Data minimization	Data minimization involves collecting only the minimum amount of data that is necessary for a given purpose	Data minimization leads to increased risks of privacy breaches and exposure of personal information
Social Engineering attacks	Refers to manipulating users to compromise the security of IoV network	Leads to unauthorized access of sensitive data, it also compromises the security credentials.

DISCUSSION AND FUTURE RESEARCH

The research has explored the critical security and privacy challenges faced within the Internet of Vehicles (IoV) ecosystem. The interconnected and dynamic nature of IoV systems introduces various issues, including unauthorized access, Sybil attacks, denial of service (DoS) attacks and data breaches. These challenges threaten the confidentiality, integrity, and availability (CIA) of vehicular data, leading to misinformation, and traffic disruptions,

affecting the users' safety. Privacy concerns such as location tracking and identity disclosure lead to trust issues and raise ethical questions about data usage and consent. The study highlights the pressing need for the development of robust models for enhancing the confidentiality, integrity, and availability of IoV systems.

To address the identified challenges and advance the field of IoV security and privacy, the following research directions are proposed for further research: 1) Advanced Authentication Mechanisms: Research should focus on the development of advanced authentication mechanisms that are robust against impersonation attacks while being scalable to accommodate the dynamic nature of IoV systems. Blockchain-based solutions that utilize distributed ledger technology for secure and transparent identity management need to be adopted in these advanced authentication mechanisms. 2) Advanced AI and ML Security in IoV: Future research studies should focus on techniques for detecting and mitigating the various IoV attacks. This can include real-time anomaly detection systems that can identify malicious activities in vehicular networks. 3) Resilient and Decentralized Blockchain Architectures: Decentralized IoV architectures that utilize blockchain and edge computing can strengthen resilience against common attacks such as DoS attacks. Future research should focus on optimizing solutions through improved decentralization strategies. 4) Simulations and Real-World Testing: Future research should focus on the development of detailed simulation environments and executing pilot projects to evaluate and validate the proposed solutions in real-world situations. These tests will help in customizing solutions that meet the scale, are easy to integrate with other systems, and accepted by users.

CONCLUSION

In conclusion, this paper investigated the security and privacy issues in the Internet of Vehicles (IoV), an exciting and rapidly growing field that connects vehicles, infrastructure, and other entities to create smarter and safer transportation ecosystem. The study has identified key threats, including Sybil attacks, denial of service (DoS) attacks, location spoofing, and eavesdropping, which compromise the confidentiality, integrity, and availability of IoV systems. Additionally, privacy concerns such as location tracking, identity disclosure, and social engineering attacks pose significant risks to user data and trust. The research emphasizes the need for advanced security mechanisms, including blockchain-based solutions, AI-driven anomaly detection, and decentralized architectures. Addressing these challenges will pave the way for the IoV to evolve into a robust, intelligent transportation ecosystem that enhances road safety, optimizes traffic management, and fosters trust among users and stakeholders. Future innovations should focus on integrating cutting-edge technologies to ensure a secure, efficient, and privacy-preserving IoV framework.

References

[1] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using Ethereum," *Sensors*, vol. 20, no. 14, p. 3928, 2020.

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[3] K. Angrishi, "Turning internet of things (IoT) into internet of vulnerabilities (IoV): IoT botnets," *arXiv preprint arXiv:1702.03681*, 2017.

[4] M. A. Al-Shareeda and S. Manickam, "A systematic literature review on security of vehicular ad-hoc network (VANET) based on veins framework," *IEEE Access*, vol. 11, pp. 46218–46228, 2023.

[5] X. Ma, C. Ge, and Z. Liu, "Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture," in *Proceedings of the International Conference on Network and System Security*, Sapporo, Japan, 2019, vol. 11928, pp. 336–351.

[6] R. Gasmi and M. Aliouat, "Vehicular ad hoc networks versus Internet of Vehicles - A comparative view," in *2019 International Conference on Networking and Advanced Systems (ICNAS)*, 2019, pp. 1–6.

[7] V. Kumar, R. Ali, and P. K. Sharma, "IoV-6G+: A secure blockchain-based data collection and sharing framework for Internet of Vehicles in a 6G-assisted environment," *Vehicular Communications*, vol. 47, p. 100783, 2024.

[8] S. A. Elsagheer Mohamed and K. A. AlShalfan, "Intelligent Traffic Management System Based on the Internet of Vehicles (IoV)," *Journal of Advanced Transportation*, vol. 2021, pp. 1–23, 2021.

[9] E. Alalwany and I. Mahgoub, "Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions," *Sensors*, vol. 24, no. 2, 2024.

[10] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693–713, 2020.

[11] K. Kaltakis, P. Polyzi, G. Drosatos, and K. Rantos, "Privacy-preserving solutions in blockchain-enabled Internet of Vehicles," *Applied Sciences*, vol. 11, no. 21, p. 9792, 2021.

[12] M. Li, J. Weng, A. Yang, J. N. Liu, and X. Lin, "Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11248–11259, 2019.

[13] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," *Cleaner Engineering and Technology*, vol. 8, p. 100481, 2022.

[14] S. Nagpal, A. Aggarwal, and S. Gaba, “Privacy and security issues in vehicular Ad Hoc networks with preventive mechanisms,” in *Proc. Int. Conf. Intell. Cyber-Phys. Syst. (ICPS)*, Singapore: Springer Nature Singapore, 2022, pp. 317–329.

[15] E. F. Cahyadi, T. W. Su, C. C. Yang, and M. S. Hwang, "A certificateless aggregate signature scheme for security and privacy protection in VANET," *International Journal of Distributed Sensor Networks*, vol. 18, no. 5, 2022.

[16] S. Azam, M. Bibi, R. Riaz, S. S. Rizvi, and S. J. Kwon, "Collaborative learning based sybil attack detection in vehicular ad-hoc networks (VANETs)," *Sensors*, vol. 22, no. 18, p. 6934, 2022.

[17] J. Su, R. Ren, Y. Li, R. Y. Lau, and Y. Shi, "Trusted blockchain-based signcryption protocol and data management for authentication and authorization in VANETs," *Wireless Commun. Mobile Comput.*, vol. 2022, Art. no. 123456, Advance online publication. [Online]. Available: https://doi.org/10.1155/2022/123456

[18] M. M. Hamdi et al., "Effect Sybil attack on security Authentication Service in VANET," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022, pp. 1–6.

[19] N. Jaya Krishna and N. Prasanth, "An Insight View on Denial of Service Attacks in Vehicular Ad Hoc Networks," in *Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2021*, Singapore: Springer Singapore, 2022, pp. 273–285.

[20] R. Sedar, C. Kalalas, J. Alonso-Zarate, and F. Vázquez-Gallego, "Multi-domain denial-of-service attacks in Internet-of-Vehicles: Vulnerability insights and detection performance," in *Proc. 2022 IEEE 8th Int. Conf. Netw. Softwarization (NetSoft)*, 2022, pp. 438–443.

[21] R. Shrestha, H. Guerboukha, Z. Fang, E. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nat. Commun.*, vol. 13, no. 1, Art. no. 3045, 2022.

[22] R. Pietrantuono, M. Ficco, and F. Palmieri, "Survivability analysis of IoT systems under resource exhausting attacks," *IEEE Trans. Inf. Forensics Security*, vol. 2023, Advance online publication.

[23] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "GPS spoofing detection via crowd-sourced information for connected vehicles," *Comput. Netw.*, vol. 216, Art. no. 109230, 2022.

[24] G. G. Shayea, D. A. Mohammed, A. H. Abbas, and N. F. Abdulsattar, "Privacy-aware secure routing through elliptical curve cryptography with optimal RSU distribution in VANETs," *Designs*, vol. 6, no. 6, Art. no. 121, 2022.

[25] Y. Liang, Y. Liu, and B. B. Gupta, "PPRP: preserving-privacy route planning scheme in VANETs," *ACM Transactions on Internet Technology*, vol. 22, no. 4, pp. 1–8, 2022.

[26] M. S. AlMarshoud, A. H. Al-Bayatti, and M. S. Kiraz, "Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures," *Vehicular Communications*, vol. 36, p. 100490, 2022.

[27] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Transactions on Intelligent Transportation Systems*, Advance online publication, 2023.

[28] M. A. Malek, "Bigger is always not better; less is more, sometimes: The concept of data minimization in the context of big data," *Eur. J. Priv. Law Technol.*, vol. 1, p. 212, 2021.

[29] R. M. Raut and S. Asole, "A survey on security threats in VANET and its solutions," in *Proc. Int. Conf. Recent Trends Artif. Intell. IoT*, Cham, Switzerland: Springer Nature Switzerland, 2023, pp. 229–240.