Advancements and Cybersecurity Strategies in V2X Communication and Transport System for Electric and Connected Vehicles Using IoT and AI

Hema Muniyappan[1], Pavithra Sankarappan[1], La Ode Muhram[2], Muhamad Farih[3], Aarthi Saravanaperumal[4], Shubham Sharma[5] and Arkan Adnan Imran[6]

[1] *Department of Computer Science and Engineering, Chennai Institute of Technology, 600069 Chennai, India*

[2] *Department of Law Science Study Program, Universitas Sulawesi Tenggara, 93116 Kendari, Indonesia*

[3] *Department of Digital Business Study Program, Universitas Sulawesi Tenggara, 93116 Kendari, Indonesia*

[4]*Center for Advanced Multidisciplinary Research and Innovation, Chennai Institute of Technology, 600069 Chennai, India*

[5] *Center for Research Impact and Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, 140401 Punjab, India*

[6]*Department of Computer Engineering Techniques, Dijlah University College, 10052 Baghdad, Iraq*

Hemam.cse2022@citchennai.net, pavithras@citchennai.net, laodemuhram@un-sultra.ac.id, muhammadfarih@un-sultra.ac.id, , aarthis.chem@citchennai.net, shubham543sharma@gmail.com, arkan.adnan@duc.edu.iq

Keywords: Vehicle-to-Everything, Automated Vehicle, V2X Communication, Bank Digital Transformation, Cloud Computing, Cyberattacks, V2X Security.

Abstract: Vehicle-to-Everything (V2X) communication has emerged as one of the transformative technologies that the automobile sector needs: it concerns with present day exchange of information between two or more vehicles, facilities, and anything that aims at enhancing safety on the roads, flow of traffic and driving in general. According to the specifications provided by 5G, edge computing, and IoT in V2X systems, the EVs gain the development opportunity of collision avoidance, traffic optimization, and energy management. On the other hand, these developments brought forward cybersecurity weaknesses: and the jamming and spoofing attacks and DDoS attacks with which reliability and safety of V2X systems is threatened. In the present paper, the particular attention will be given by the author to outlining the newest technology trends and cyber security frameworks responses to the threats found in defending the channels in the V2X system– current and future. It lists relatively broad topics as the following general topics: authentication schemes applicable for V2X networks, encryption techniques that can be used in V2X communication link, and IDS system that can be implemented for V2X networks. More importantly, it demonstrates how AI can enhance the security of the vehicular network and realistic legislation may construct a foundation for V2X cyber security. This work explains research toward developing a secure V2X environment for readiness in integrated transport system with safer, efficient and sustainable methods.

1 INTRODUCTION

Smart cities use ICTs in economy, environment, and social spheres, solving urbanization issues with new technologies [1]. Smart city services secured $80 billion in 2018 compared to $67 billion in 2017 and expected to reach $135 billion in 2021 (IDC Research). Main investments concern ITC for transport, and environmentally friendly transport systems, though regional. The US and Europe are most concerned with transport while China is concerned with watching citizens through cameras and Japan – with environmental control. The US and China are the biggest [2] spendings with $22 billion and $21 billion respectively in context with the Vehicle-to-Everything Communication for Electric and Connected Vehicles. In accordance with the smart cities with the transformative contemporary technologies in relation with the enhancing road safety and transport system is centered, the IoT solutions are predominant in smart city solutions and the overall global IoT expenditure is estimated to touch 123.8 Billion US dollars in the year 2021.

IoT extends value and disrupts the conventional industries especially the transport industry due to enhanced detection, Artificial Intelligence, and data analysis. The Spanish Recommendations for IoT show this growth; connected objects are predicted to reach 5 million in 2018 and 8 million by 2022 Vehicular communication, which includes V2X (Vehicle-to- Everything), I2X (Infrastructure-to-Everything), and P2X (People- to-Everything), is for smart mobility [3] though much work has been done on V2X, new communications such as I2X and P2X have not found standards. Present work examines industrial and scientific developments, bibliometrics and future targets from the major scientific databases with regard to further development of essentials for smart cities as the global population increases the demand put on them [4]. Figure 1 shows that the advantages of the smart citizens that leverage ICTs to enhance economic, environmental, and social aspects, addressing urbanization challenges through innovative technologies.

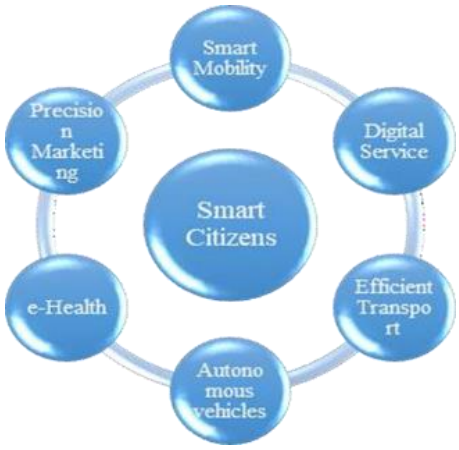

Figure 1: Advantages of smart citizens that influence ICTs to strengthen the technologies including the transport industry by using AI-IoT.

2 ADVANCES IN V2X COMMUNICATION TECHNOLOGIES

The progress in Vehicle-to-Everything (V2X) technology, focusing specifically on the future of transportation system and collaboration between vehicles, infrastructure [5], and their users with referenced real-time data sharing. This is highlighted by early research into banking and cloud security highlighting its early-stage evolution and covering both risks such as phishing and malware as well as newer frameworks [6] such as MFA and hybrid cloud security. In the mid-2010s, there is blockchain for secure transaction and CASB for security management of the cloud vulnerabilities; in the late 2010s, it is AI- enabled fraud detection and the security concept zero-trust [7]. Although comparatively small, the trends emerging point to a future where IoT, quantum-safe cryptography, and biometric behaviors will be dominant and will require adaptable solutions [8].

Additionally, the study identifies areas of future development like the combination of AI and IoT for infrastructure in smart cities, quantum-proof cryptography for emerging banking applications. V2X security protocols that use such elements like encryption and etc. are critical to solving cybersecurity issues such as spoofing and DDoS attacks. Highlighted in the survey, V2X system protection requires effective frameworks and international cooperation; problems call for legislation, AI-based anomaly recognition, and blockchain-based data accuracy. The goal of this work is therefore to create a safe environment for V2X that leads to improved, safer, efficient and sustainable transport systems while at the same time considering emerging new trends in cybersecurity risks [9].

2.1 Unaddressed Challenges in V2X Technology

While AI and IoT are pivotal to smart cities, research lacks practical solutions for their secure integration. Issues like real-time data processing, scalability, and privacy remain underexplored, particularly in urban infrastructures. As hybrid and multi-cloud models expand in smart cities and banking, detailed insights into their unique security challenges are missing. Critical issues such as secure data synchronization, distributed access control, and interaction between public and private clouds need further study. Although promising, behavioral biometrics face limited research on their scalability and adoption in banking systems [10]. Additionally, ransomware attacks in cloud-hosted systems lack proactive and sector-specific detection frameworks. Despite growing awareness of quantum threats, there is insufficient research on transitioning banking and IoT systems to quantum- resistant cryptographic methods [11].

2.2 Applications of AI-IoT Technologies for Road Safety and Intelligent Transport in Smart Cities

The methodology of this review is to stand back and aim to look how key gaps in the literature can be improved when discussing cybersecurity issues and innovations in smart cities and cloud banking. This research investigates the application of AI-IoT technology in smart cities with particular focus on technical and privacy concerns in practice-based settings. Its purpose is to present the challenges related to security and data management in the systems based on hybrids and multi-clouds in both the urban and financial environments for building complex multimodal infrastructures [12]. Further attention will be paid to the use of quantum immunity in banking and Iot networks and possible transition from traditional cryptographic system to quantum immune. In addition to this, the review shall assess open proactive measures against ransomware in cloud infrastructure and use of behavioral biometrics for banking user identification. Pointing out these key challenges and the related actionable solutions, the present review should act as the basis for further research and enhanced security approaches to these very remarkable domains [13].

3 MATERIALS AND METHODOLOGY

Banking and cloud computing digitization creates highly advanced dangers with strong persisting threats, ransomware attacks, and insider attacks on the banking sector. In the banking industry, APTs target financial transactions [14]. On the other hand, ransomware attacks occurs frequently against cloud-hosted applications while exploiting shared environment vulnerabilities. Such threats point toward having a proactive defense system specially customized for each sector.

Figure 2 shows that the different types of threats of the evolving cybersecurity threats. Digitalization of banking, cloud computing results into high protection of advanced, continuous threats, ransomware, insider's threats to banking. In the banking industry the threat is done towards the financial transaction by APTs [15]. On the other hand, ransomware attacks are prevalent on the cloud hosted applications due to the reasons they exploit the shared environment vulnerabilities. Of course, such threats indicate that there should be a preemptive defense strategy and this further should be industry specific. The use of algorithms for the attribute recognition of patterns and comparison of the obtained data with reference information contributes to the more efficient search for signs of risk and the use of outsourcing with cybersecurity companies for penetration Testing no more than once a year to ensure that hidden vulnerabilities of cloud infrastructures are revealed. Making systems more secure is the key reason preparing them for premium challenges by using protocols such as quantum-resistant algorithms [16]. The data transmission and storage, where a multilayer security system-including, endpoint security and Secure Application Program Interface-was attempted to lower risks. This makes the security policy always check and updated, thus, be strong enough to manage with the new form of attack of by hackers.

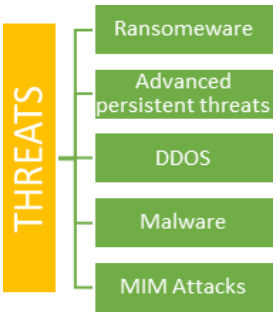

Figure 2: Different types of threats, including cybersecurity threats.

3.1 Enhanced Defense Protocols for V2X Communication in Connected and Autonomous Vehicles Using AI–IoT Technologies

V2X communication systems herald positive change in connected and autonomous vehicle systems enhanced by advanced technologies. V2X protocols incorporate 5G in the communication between vehicles and infrastructures and IoT for edge computing and integrated information sharing, primarily for the safety of life, property, and better traffic and energy management. V2X communication systems are introducing positive development and innovation in connected and autonomous applications enabling sophisticated technology. 5G and V2X, V2X hit control operate 5G [7] in the vehicle and infrastructure communication, and IoT governs the edge computing and the coordinated data exchange, mostly for safety of lives and property, efficient traffic, and energy usage. More effective encryption

and stronger privacy preserving pseudonym schemes also strengthen the defenses, which gets the communication secured and users' identities safeguarded. The integration of these protocols evidences that V2X systems can enhance safer, smarter and more sustainable transportation Systems is shown in the Table 1.

The existing V2X communication systems have transformed the fields of connected and autonomous vehicles with the help of technologies such as 5G and IoT to allow data transfer. These protocols had contributed to the improvement of traffic flow, energy usage and safety. Secure communications and privacy protection of user identity entail the use of sound encryption regimes, pseudonymity, and privacy-preserving measures. Also, AI and machine learning are critical in the V2X since they are used in alarming of anomalies or prognostication of likely system failure. Some of the benefits of predictive maintenance using AI include: cutting on time that could have been spent repairing or replacing components that are down. Blockchain core concepts [8], such as decentralization and anonymity, improve the reliability of data, as well as decrease fraudulent scenarios, thanks to an effective record of data partitions. The integration of 5G network slicing assures separated pathways and robust shields against cybersecurity threats to specific services. Everyone knows that firmware updates and patches are made periodically to protect systems from new risks. This allows automakers, regulators and tech providers to standardize the security platforms and entwine the defenses creating healthy and secure integration that protected the constantly transforming transportation systems.

3.2 Regulatory Compliance and Identity Management in V2X Systems

There is strong security that identifies and protects the vehicles from being accessed by unauthorized persons:

- Intrusion detection systems or simply IDS. These systems keep observing the vehicular communication for irregularities and threat.
- Regulatory compliance. GDPR compliance, as well as the use of the Zero Trust model and standards that are specific to V2X, allow for the alignment of cross-border security. These advances bear to the development of robust V2X systems to support safer, smarter, efficient, and sustainable transportation systems.
- Regulatory compliance in cybersecurity.

Protocols like GDPR, PCI DSS, and Zero Trust security model are necessary for protection of such data. Cloud providers and banks are protected for data control and transfer across borders by the GDPR regulation. Sequential verification of user identities used in Zero Trust strategies is essential for combating insider threats in contexts of hybrid cloud. Furthermore, it also confirms with the compliance and operational security in the cloud banking and also integrates the strong identity access management system. Cybersecurity compliance is vital for cushioning Hybrid Cloud-Specific in addition to banking security against risks, it makes sure security of vital information. Being in line with international standards like ISO 27001 makes it easy to combat cross border issues since measures are standard worldwide. Not only compliance with these standards can be observed in result of regular audits, but also potential threats can be identified on time.

Table 1: Key features and technologies in V2x communication.

Technology	Application	Benefits	References
AI and Machine Learning	Anomaly detection, collision avoiding	It enhances safety and the possibility of the right route planning.	[1] [8] [15] [9] [2]
Blockchain	Ensuring security for the exchange of vehicular data	The work of this layer is to maintain the accuracy of the data as well as reduce the risk of fraud.	[3] [10] [7]
Advanced Encryption	ECC and post – quantum security is Among the cryptographic protocols that need to be reconsidered in new communication networks	It improves the communication security.	[5] [6] [10] [11] [14] [2]
Privacy Mechanisms	Pseudonym- based frameworks	Protecting users' identification and their data	[12] [7]

Dissemination of complicated compliance frameworks should therefore be elastic in the face of constant cyber threats in order to improve organizational security. Industry, cloud providers together with the financial sector and the regulatory board develop synergy strategies to enhance compliance and security. In the same way, industry-specific frameworks in handling incidents reduce the loss of time due to the prompt restoration from the breach. Thorough training of the users makes awareness on TOP threats, and prevents insider threats, and strengthens identity and access management initiatives. These strategies in synergy work to align compliance measures with operational security [9] opening the doors to safer, smarter, and more efficient systems. To expand on the level of regulatory compliance, new and higher sophisticated risk management instruments are implemented into an organization that ensures that the compliance assessment is conducted concurrently with work. Both tools are particularly useful for understanding the existing security gaps and improving the processes of remediation. It is possible to safely achieve compliance by implementing SASE architecture in cloud-first designs that provide comprehensive network security. Moreover, work in accordance with the concept of an immutable audit trail enhances accountability that, in turn, contribute to better tracking and reporting of compliance activities. Working closely with the regulatory authorities and being a member of the compliance-based consortiums help organizations to be ahead in the current emerging policies. In addition, using various forms of encryption depending on the conditions in a country when transferring data across borders meets different needs. AI and machine learning are also slowly being used to fully automate compliance checks so that these can be checked in real time. Thus, the last element of the framework is promoting the transparency with stakeholders and issuing regular compliance reports that would create trust and show the continuing work on the cybersecurity best practices.

Figure 3: Types of V2X communication.

Figure 3 shows that the types of V2X communication that is used in the Compliance frameworks like GDPR, PCI DSS, and Zero Trust models are vital for securing sensitive data. It integrates robust identity access management systems ensures compliance and operational security in cloud banking for adjacent cooperation and energy efficient methods like platooning by giving additional information to the self-driving vehicle [2]. V2X is also useful to emergency response systems by providing priority to emergency vehicles and to notify other drivers to facilitate time reduction and safe operation. Besides, it has enhanced the users' experience, real-time information in terms of parking space and road status, and interacting with smart city systems in order to make the right pre-planned travel. This technology helps to encourage better, safer, and efficient means of moving people from one place to another as shown in the Table 2.

Table 2: Different V2X communication types.

V2X connectivity type	Description	References
V2I| Vehicle to Infrastructure	Cars and road infrastructure (traffic lights, road signs, parking lots, etc.)	[1], [5], [8], [9], [12]
V2P | Vehicle to Pedestrian	Cars and pedestrians	[10], [15]
V2V| Vehicle to Vehicle	Vehicle(car) to vehicle (car)	[8], [11]
V2N| Vehicle to Network	Vehicle (car) and networks	[1], [4], [5]

Compliance is crucial to the matters of data confidentiality and organizational security, most/values-of-all especially in case of the usage of hybrid cloud services and the banking sector. The setup of GDPR and implementations such as the PCI DSS provide strong systems for controlling data flow across borders establishing increased relevance due to the increase in international cooperation. Sequential verification processes in the recommendations of the Zero Trust security models are successful in identifying insider threats.

Additionally, compliance measures developed for the specific sector for the financial and transport sector tackle specific needs. Security measures like the multi-factor authentication do improve trust within the user base. Automized compliance check guarantees that the program continues to observe on regulations even as systems change. Technologies such as homomorphic encryption enable computation on data in a manner that legislation compliance and

anonymity of patients can be maintained. Contracts facilitate and promote cooperation and the functioning of multiple systems that connect countries. Also, once adopted, the internal and external audits together with adaptive security measures, provide a flexible work environment that addresses the ever-evolving nature of cyber risks and enhances the protection of compliance operations.

3.3 Benefits of V2X Communication

V2X stands for Vehicle to Everything and it is an advanced system out in transportation sector whereby the vehicles and other entities such as infrastructure, people on the ground and other networks exchange data and information in real time manner. Through collision warnings, alerts to pedestrians, and assistance for lane changing, V2X has gone ahead to enhance traffic safety by Avoiding Accidents leading to tremendous improvements in accident rates. Enhanced traffic flow provides the smart traffic control option, changes to dynamic roads, and even low traffic density in traffic as the result of less fuel utilization and pollution. It is applied to resolve the challenges of the vehicular environment

4 RESULTS AND DISCUSSION

This paper is a review paper which involves a review of review papers with regard to the dynamic security environment in the banks and cloud computing frameworks. This it attributes to rise digitalization and mode complex forms of cyber threats. Among all the identified findings, the following can be highlighted: increased incidence of ransomware techniques, phishing, insider threats, and APT in the financial structures and customer databases. Misconfiguration particularly of popular resources in cloud architectures and ransom attacks are considered as threats in the cloud structures paradigms of defenders have been defined with use of artificial intelligence and machine learning in the identification of fraudulent and other behaviours in real-time. Besides, Cyber threat intelligence frameworks are available that can definitively assist in recognizing threat and control risks before they can harm the organization and become normal procedure over cloud banking data integrity through blockchain technology at on- boarding stage. NIST CSF and ISO/IEC 27001 have equally assisted in enhancing structure to CSI especially in HC environments; still, researchers lack works exploring cross-border compliance of CSI and its integration with Zero Trust models. Some of these issue have been debated many of them have been addressed however, problems such as, how to scale AI, how to prevent malicious insiders, and how to move to quantum safe cryptography prove that there is still much more to achieved. It is necessary that there should be more development and collaboration to mitigate cyber threats on banking and cloud computing today and in the future. This paper also highlights the increasing need to involve robust cybersecurity strategies in current and upcoming technologies such as V2X communication. In view of advancement and adoptions of connected and autonomous vehicles, real-time anomaly detection, secure encryption, and data exchange technologies are inevitable. Blockchain technology has been cited to have advantages on cloud banking and thus can be adopted and enhanced to fit vehicular networks on aspects of data integrity and availability. Additionally, by widely implementing AI and ML in vehicular systems, it is possible to dramatically enhance the possibility of identifying and mitigating cyber threats on the fly. Thus, the protection of the existing systems and development of the effective strategies for a further attack requires the international cooperation in the sphere, the easing of the international regulations, the transition to the quantum-safe cryptography.

V2X communication facilitates exchange of information between vehicles, infrastructure, and peds in near-real time; hence – increases road safety and operational efficiency. Highlights such as the collision system, pedestrian sensing system, and a lane change system decrease the levels of accidents and enhance transportation safety. V2X improves traffic conditions through the initiation of route changes and the provocation of less traffic density, and better fuel consumption. In addition, V2X complements other advanced technologies such as IoT in the provision of smart navigational networks as well as efficient use of energy in the vehicle. Real-time weather and road condition information make a driver's decision-making process reliable by improving journey reliability. Platooning in combination with V2X boosts up fuel efficiency and decreases the number of carbon emissions due to coordinated movement of vehicles. In emergency response systems, priority routing gave fastest routes to ambulance and fire trucks which reduce response time. Furthermore, through machine to machine communication, V2X improves driver experience provisions such as parking spaces, traffic conditions, and compatibility with smart city services. All these advancements bring safety, intelligence and sustainability to transport, fostering mobility for the future.

5 CONCLUSIONS

V2X is one of the transformative ways, and its application laid down significant aspects in safety, efficiency in transportation and sustainability. It can permit experience to data exchange between vehicles, infrastructure, and pedestrians and reduce as many of the accidents as possible. Also, in turn, it would help to optimise traffic management. It is also future-ready since it can work together with other sophisticated systems like AI, and IoT so that it can tackle problems that are still going to occur with vehicle coordination and emissions. V2X is environmentally friendly: That reduces the use of fuel and emission in dynamic route finding, and the other cooperative driving methods like the leading and following formation. The technology is important in Emergency Response Systems since it increases efficiency in the execution of these operations through traffic prioritized services to emergency vehicles. Essentially, efforts to standardised V2X protocols require collaboration between governments, automotive industries and smart city designers at a national and international level and across manufacturers. To ensure public acceptance of the gain from the smart transportation systems, V2X-secure communication needs to be continuously researched and imbibed and investment is to be made regarding the cybersecurity and data integrity concerns.

ACKNOWLEDGEMENT

This work is partially funded by Center for Advanced Multidisciplinary Research and Innovation. Chennai Institute of technology, India, vide funding number CIT/CAMRI/2025/CFR/010.

REFERENCES

[1] D. G. Costa, J. C. N. Bittencourt, F. Oliveira, J. P. J. Peixoto, and T. C. Jesus, "Achieving sustainable smart cities through geospatial data-driven approaches," Sustainability, vol. 16, no. 2, p. 640, 2024, [Online]. Available: https://doi.org/10.3390/su16020640.

[2] K. I. Shah, M. Khan, S. Abbas, and Z. Hasan, "Intelligent transportation system (ITS) for smart-cities using Mamdani fuzzy inference system," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 2, p. 105, 2018, [Online]. Available: https://doi.org/10.14569/IJACSA.2018.090215.

[3] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang, Y. Xiang, and S. Yu, "An overview of attacks and defences on intelligent connected vehicles," arXiv preprint arXiv:1907.07455, 2019, [Online]. Available: https://arxiv.org/abs/1907.07455.

[4] S. Yogarayan, S. F. A. Razak, A. Azman, and M. F. A. Abdullah, "Vehicle to everything (V2X) communications technology for smart mobility in Malaysia: a comprehensive review," J. Southwest Jiaotong Univ., vol. 56, pp. 534-563, 2021, [Online]. Available: https://doi.org/10.35741/issn.0258-2724.56.4.47.

[5] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," Proc. IEEE, vol. 110, pp. 712-734, 2022, [Online]. Available: https://doi.org/10.1109/JPROC.2022.3173031.

[6] T. Butt and M. Afzaal, "Security and privacy in smart cities: Issues and current solutions," in Smart Technologies and Innovation for a Sustainable Future, pp. 317-323, 2019, [Online]. Available: https://doi.org/10.1007/978-3-030-01659-3_37.

[7] I. H. Abed and S. Bahadori, "Using density criterion and increasing modularity to detect communities in complex networks," IJDS, vol. 2, no. 1, pp. 1-15, Jan. 2025, [Online]. Available: https://doi.org/10.62051/ijds.v2i1.15.

[8] K. Ahmad, "Internet of Things-aided intelligent transport systems," Wireless Commun. Mobile Comput., vol. 1, no. 1, p. 28, 2023.

[9] K. Ansari and Y. Feng, "Design of an integration platform for V2X wireless communications and positioning supporting C-ITS safety applications," J. Glob. Position. Syst., vol. 12, pp. 38-52, 2013, [Online]. Available: https://doi.org/10.5081/jgps.12.1.38.

[10] J. Clancy, D. Mullins, B. M. Deegan, and J. Horgan, "Wireless access for V2X communications: Research, challenges and opportunities," IEEE Commun. Surv. Tutor., 2024, [Online]. Available: https://doi.org/10.1109/COMST.2024.3384132.

[11] T. Wang, A. Hussain, X. Wang, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: A survey," IEEE Access, vol. 7, pp. 1-1, 2019, [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2891073.

[12] M. Houmer, "A secure vehicle to everything (V2X) communication model for intelligent transportation system," Comput. Intell. Recent Commun. Netw., vol. 1, no. 1, p. 102, 2022.

[13] S. A. Yusuf, A. Khan, and R. Souissi, "Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety," Transp. Res. Interdiscipl. Perspect., vol. 23, no. 11, p. 100980, 2024, [Online]. Available: https://doi.org/10.1016/j.trip.2023.100980.

[14] M. S. Alsabah, N. M. A. Aljarah, and S. V. Paşca, "Intelligent algorithmic approaches to ECG signal classification in heart disease detection," Electr. Eng. Tech. J., vol. 2, no. 1, pp. 25-32, Jan. 2025.

[15] K. Kim, J. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Comput. Secur., vol. 103, p. 102150, 2021, [Online]. Available: https://doi.org/10.1016/j.cose.2020.102150.

[16] T. Yoshizawa, D. Singelée, J. Mühlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in V2X communication systems," ACM Comput. Surv., vol. 55, no. 9, p. 35, 2023, [Online]. Available: https://doi.org/10.1145/3558052.