Indonesian Journal of Electrical Engineering and Computer Science
Vol. 35, No. 1, July 2024, pp. 213~221
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v35.i1.pp213-221

Artificial intelligence powered internet of vehicles: securing connected vehicles in 6G

Depa Ramachandraiah Kumar Raja[1], Zuraida Abal Abas[1], Chandra Sekhar Akula[2], Yellapalli Dileep Kumar[3], Goshtu Hemanth Kumar[4], Venappagari Eswari[4]

[1]Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[2]Department of Computer Science Engineering, Avanthi Institute of Engineering and Technology, Vizianagaram, India
[3]Departement of Electronics and Communication Engineering, School of Engineering, Mohan Babu University, Tirupati, India
[4]School of Electronics and Communication Engineering, REVA University, Bengaluru, India

Article Info

Article history:

Received Dec 14, 2023
Revised Feb 9, 2024
Accepted Mar 14, 2024

Keywords:

6G network
Anomaly detection
Deep learning
Internet of vehicles security
Machine learning
Vehicle-to-everything

ABSTRACT

The rapid advancements in automotive technology and the emergence of next-generation networks such as 5G and 6G are laying the foundation for the internet of vehicles (IoV), a revolutionary concept to transform transportation systems. The convergence of artificial intelligence (AI) and connected vehicles IoV is driving a paradigm shift in the transportation sector, especially in the dynamic framework of 5G and future 6G networks. This survey paper provides a thorough survey of the evolving AI-based IoV security landscape. We explore key areas of 5G/6G networks, focusing on the complex interplay of machine learning (ML) and deep learning (DL) in enhancing vehicle-to-everything (V2X) security and connected vehicles. Addressing the unique challenges of 6G, this paper outlines future directions for improving security and highlights open research issues. This comprehensive survey, which aims to provide information and guidance to both researchers and practitioners, contributes to a detailed understanding of the security issues associated with connected vehicles in the emerging 6G era.

Corresponding Author:

Zuraida Abal Abas
Faculty of Information and Communications Technology, Universiti Teknikal Malaysia Melaka
Melaka, Malaysia
Email: zuraidaa@utem.edu.my

1. INTRODUCTION

The development of vehicular communication systems has been transformed into the concept known as the internet of vehicles (IoV), which is a result of fast-evolving car technologies and upcoming 5G and 6G networks [1], [2]. In recent years, with the convergence of artificial intelligence (AI) and advanced communication networks, the automotive industry has entered a new era of intelligent connected vehicles IoV. This journey of change triggered by the transition from 1G to 5G has witnessed an unprecedented convergence of cutting edge technologies that promise improved safety, efficiency, and personalized experiences in the automotive industry [3]. The intersection of AI and intelligent connected vehicles (IoV) has the potential to revolutionize not just our modes of transportation, but also the structure of our entire transportation system. This article provides a comprehensive understanding of the evolving security landscape in AI-based IoV. As the integration of machine learning (ML) and deep learning (DL) shapes the intricacies of vehicle-to-everything (V2X) security and connected vehicles, the paper examines key areas of 5G/6G networks. The survey addresses the unique challenges posed by 6G and outlines future directions to improve security and open research issues. To contextualize this study, it is imperative to acknowledge the importance of previous work in this area. The convergence of AI and IoV has been explored by notable contributors who have laid the foundation for understanding the potential and challenges within this symbiotic relationship. Their research has provided insights into AI's capabilities in designing connected vehicle systems. However, the evolving landscape of 5G and the impending deployment of 6G networks bring new challenges that require further exploration. The current challenge is to ensure the security of AI-driven IoV systems in the ever-changing landscape of 5G and the anticipated complexities of 6G. Existing literature highlights the potential of AI in improving the functionalities of connected vehicles, but the security implications in evolving network scenarios remain insufficiently addressed. This article contributes by providing a thorough analysis of AI-based IoV security, with a specific focus on the interplay of ML and DL in V2X security. The aim is to fill the gap in the existing literature by addressing the unique challenges presented by 6G networks. By providing insights into these challenges and outlining future directions, the paper not only provides valuable information for researchers and practitioners but also strives to guide the community toward a safer and more resilient connected vehicle ecosystem in the emerging era of 6G. This article is organized as follows: section 2, the literature review, aims to provide current research in this area and provide an in-depth analysis. Section 3 describes the key areas within 5G/6G networks for AI-powered IoV. Details of the key AI algorithms and techniques used to secure V2X communications are discussed in section 4. In section 5 presents the future of AI-powered IoV security in the 6G landscape and highlights several new research directions. In section 6 describes open research questions and challenges. Finally, section 7 summarizes the conclusions drawn from the discussions throughout the article.

2. RELATED WORK

Integrating 5G networks into vehicle communication systems is crucial, providing comprehensive functionality and enabling advanced services such as secure data exchange and remote diagnostics. This literature review explores ongoing research initiatives in this area, focusing on bringing together secure communications protocols, privacy protections, and intelligent technologies in automotive networks. By assessing existing projects, this analysis aims to gain insights that can serve as a basis for future advances to ensure the optimal integration of 5G into vehicle communications in terms of efficiency, reliability, and safety. Eventually, this review aims to advance the development of automotive systems and promote the development of safer, smarter, and more connected transport ecosystems.

2.1. Secure communication protocols

5G-enabled vehicle networks (VNs) hold great promise for a transportation revolution, but they also bring new security and privacy challenges. To address these issues, researchers have proposed several innovative solutions. Al-Shareeda *et al.* [4] developed a method for exchanging data in 5G-enabled VNs without relying on roadside units (RSUs). This approach aims to reduce costs and complexity by using data aggregation techniques and simple encryption to ensure the confidentiality and integrity of the exchanged data. Ma *et al.* [5] introduced an authentication scheme that focuses on ensuring security. Their method incorporates a key management mechanism and lightweight cryptography to guarantee the integrity and security of remote diagnostic procedures. Rasheed *et al.* [6] proposed a technique that prioritizes both privacy protection and accurate information gathering. Their approach achieves a balance between user privacy and reliable data collection through aggregation methods and granular privacy controls. The researchers [7]–[10] conducted an analysis of security vulnerabilities and privacy concerns in virtual networks enabled by 5G technology. They recommended countermeasures such as intrusion detection systems, encryption, and protocols for preserving privacy during data exchange to mitigate these risks effectively.

2.2. Integration of intelligent technologies

The researchers [11]–[14] proposed an approach that improves communication security in complex vehicular environments where multiple devices generate and exchange sensitive data. Baldini [15] have proposed a framework for secure and reliable transfer learning in the context of the IoV. This framework allows knowledge to be transferred from trained models to new domains eliminating the need for extensive data collection and training. Sedjelmaci *et al.* [16] have introduced a crowd-sensing method for 5G IoV that combines deep reinforcement learning and blockchain technology to tackle these concerns. By optimizing the data collection process through reinforcement learning and ensuring the integrity and traceability of crowd-sourced data via blockchain this approach addresses the challenges effectively. Grover *et al.* [17] have proposed a network empowered by edge computing and deep learning. This architecture utilizes edge computing resources to establish security measures while leveraging deep learning algorithms for detecting anomalies and mitigating threats. In exploring edge intelligence for driving in 6G wireless systems the researchers [18]–[20] delved into the associated design challenges as well as potential solutions. These studies empha-size the importance of low latency connectivity, efficient data processing, and intelligent decision-making at the edge. The suggested solutions aim to optimize communication and intelligence deployment at the edge.

2.3. Security measures

Ibn-Khedher *et al.* [21] have proposed a scheme that combines technology with intelligent sensing to track the activities of autonomous vehicles. This integration aims to enhance the security and reliability of sensing data enabling trustworthy data exchange among autonomous vehicles. Djenouri *et al.* [22] have explored the intersection between machine learning and vehicular communication. They highlight advancements and applications in this area emphasizing the crucial role of machine learning techniques in securing communications within the IoV. Yang *et al.* [23] proposed an intrusion detection architecture empowered by AI for the IoV. Their architecture leverages AI techniques to improve intrusion detection and mitigation providing a cybersecurity solution for vehicular networks. This thorough review of the literature provided an in-depth analysis of current developments in secure communications and how to integrate intelligent technologies into automotive networks.

3. KEY AREAS IN 6G NETWORKS FOR AI-POWERED IOV

The approach of this article includes a comprehensive survey of the evolving security landscape in AI-based IoV against the dynamic backdrop of 5G and 6G networks. The central focus is on solving the complexity of ML and DL applications in V2X security and connected vehicles. An important aspect is to address the existing knowledge gap regarding the security implications of AI-driven IoV systems as we transition from 5G to the expected complexities of 6G networks. As V2X technology evolves, so do threats, requiring a proactive and adaptive approach to security. As we move into the uncharted territory of 6G networks, new horizons for AI-based IoV security challenges open up. This paper addresses these issues in detail, considering the unique characteristics and requirements of the upcoming 6G environment. It also looks to the future by providing insights into potential directionsfor AI-based IoV security in the context of 6G, anticipating changes in the threat landscape and technology paradigm as shown in Figure 1.

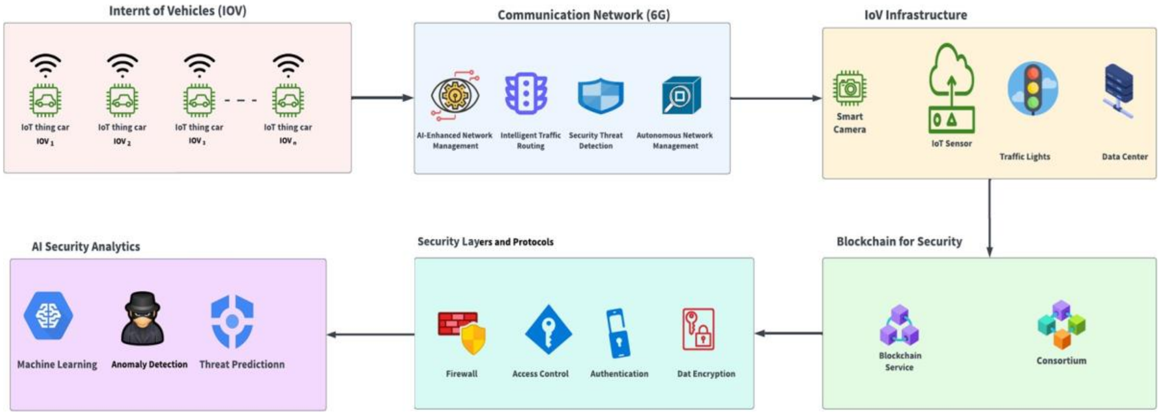

Figure 1. Security landscape of connected vehicles

The convergence of ML and DL in V2X security requires a nuanced understanding that leads to applying a tailored methodology for a detailed study of these technologies in the specific context of connected vehicles. This strategic decision is reinforced by the objective of addressing the challenges posed by 6G networks and bringing new insights and future directions to improve security measures. The methodology includes a thorough investigation, an in-depth analysis of key areas within the 5G architecture, and anticipation of the expected complexity of 6G networks. Combining 5G/6G networks with AI-based IoV can revolutionize intel-ligent transportation systems and vehicle safety. Mobile edge computing (MEC) can be combined with AI technology to process data in real-time and provide intelligent and effective IoV services [24]. The use of 6G networks facilitates the transmission of multimedia messages and videos for accident investigation and road situation detection due to high transmission rates and quality of service (QoS) guarantees [25]. Additionally, implementing edge intelligence (EI) in autonomous driving systems can offload workloads to edge servers to reduce processing costs and increase inference accuracy [26], [27]. The integration of MEC, AI, and 6G networks has the potential to create a safer and more reliable autonomous driving experience [28].

3.1. AI-optimized slicing in 6G

Network slicing in 5G means providing customized services by dividing the network into entire networks called ‘slices’. Security issues arise during the network slice life cycle, and machine learning and deep learning algorithms are used to address these issues. Using AI for network slicing can help prevent attacks, threats, and issues, and enhance the security of 5G networks [29].

3.1.1. Enhanced security in 6G

A. Scenario 1: detecting anomalies with machine learning

The primary aim is to swiftly protect connected vehicles from potential threats by detecting anomalies in their normal behavior [30], [31]. This goal is achieved by using state-of-the-art unsupervised machine learning algorithms, particularly autoencoders, which enable connected vehicles to detect anomalies in real-time. Consider a scenario where a connected vehicle is equipped with an AI-optimized slicing capability that allows it to immediately detect abnormal sensor readings that could indicate a potential cyber threat. By leveraging machine learning capabilities, the system activates an ultra-low latency communication section that enables rapid assessment and proactive measures to prevent a security breach. This advanced approach ensures that connected vehicles can respond quickly and effectively to anomalies, significantly improving overall cybersecurity in vehicle networks.

B. Scenario 2: adaptive security measures through reinforcement learning

The objective is to strengthen overall security resilience by dynamically allocating resources to changing security requirements [32]. Reinforcement learning techniques are used to achieve optimized resource allocation. The system continually adapts to new threats by learning from past security incidents. Imagine a scenario where there is a sudden increase in cyber threats in a particular region. The reinforcement learning model dynamically redistributes resources, strengthening security measures in the affected area. This adaptability guarantees a proactive response to new threats, giving you an edge against cyber criminals.

C. Scenario 3: collaborative threat intelligence with federated learning

Support collaborative threat intelligence sharing between connected vehicles with a focus on maintaining data privacy [33]. The solution lies in using federated learning models, which enable vehicles to jointly train AI models for threat detection without putting sensitive data at risk. Imagine a scenario where multiple vehicles are exposed to a new type of cyber threat. Federated learning steps in and facilitates collaborative model updates without exposing sensitive information. This powerful technique highlights the effectiveness of collaborative threat intelligence while promoting privacy protection.

3.2. AI-Enhanced security in 6G IoV

In the transition to 6G networks, particularly within the Internet of Vehicles (IoV) paradigm, AI-enhanced security emerges as a pivotal factor in ensuring the safety and stability of these evolving systems. As 5G networks lay the groundwork for 6G, integrating AI-enhanced security measures becomes imperative to fortify defense against emerging threats and vulnerabilities. The IoV, with its interconnected nature, accentuates the significance of AI-driven security protocols to safeguard communication channels, data integrity, and overall system resilience. Therefore, prioritizing developing and deploying AI-enhanced security mechanisms is crucial for establishing a robust foundation as we progress towards the era of 6G connectivity in the IoV landscape [34]. Consider the following for AI-enhanced security in the context of 5G and anticipated 6G for IoV:

3.2.1. AI-Driven threat detection

The main goal of deploying AI-driven threat detection is to leverage sophisticated algorithms for dynamic identification and real-time response to emerging threats in the IoV. The algorithm chosen for this is deep learning for anomaly detection. Within the IoV network, deep learning models, a subset of machine learning, play a central role in continuously analyzing network behavior [35]. These models excel at recognizing typical operational patterns and detecting anomalies such as unusual data flows or unauthorized access attempts. In this way, they contribute significantly to mitigating potential security threats, including cyberattacks, and ensuring the protection of the IoV ecosystem.

3.2.2. Secure multi-access edge computing (MEC) with AI integration

The integration of AI into the MEC architecture aims to establish secure, low-latency processing at the edge of the IoV. An innovative strategy in this context is federated learning, which enables joint training of AI models by edge devices within the IoV without compromising sensitive data [36]. This collaborative learning approach increases security by protecting privacy while enabling edge devices to collectively detect and combat emerging threats. This makes the IoV network more secure and responsive.

3.2.3. AI-optimized authentication and authorization

Improve user and device authentication by implementing intelligent adaptive mechanisms based on AI [37]. Behavior-based authentication uses AI algorithms to consistently analyze and adjust authentication levels in response to historical patterns of user or device behavior. This dynamic approach significantly increases security by quickly identifying potential anomalies and adjusting authentication mechanisms accordingly. This increases the overall security of the IoV network.

4. SECURING V2X COMMUNICATIONS

Connected V2X communications play a vital role in modern transportation systems. To ensure the integrity, privacy, and reliability of data exchange, advanced security mechanisms powered by AI are utilized [38]–[40]. As we move from the era of 5G to the anticipated 6G, it is expected that the security landscape for V2X communications will evolve. The details of the key AI algorithms and techniques deployed in securing V2X communications.

4.1. Machine learning-based anomaly detection algorithm: Anomaly detection for traffic patterns

The primary objective of this algorithm is to identify deviations from normal traffic patterns in V2X communications. Machine learning algorithms, particularly those employing unsupervised learning, analyze historical traffic data to learn normal patterns [41], [42]. These models can detect anomalies such as sudden traffic increases or unusual message volumes, allowing for timely alerts to potential attacks.

Case study: let’s imagine a scenario where an anomaly detection system is deployed in a smart city’s V2X network. In this situation, the system detects an abnormal surge in message frequency, which indicates a potential distributed denial of service (DDoS) attack. To safeguard uninterrupted V2X communication, the system triggers countermeasures that effectively mitigate the attack.

4.2. Deep learning-based intrusion detection algorithm: Intrusion detection with deep neural networks

The objective of this algorithm is to classify V2X messages as either benign or malicious based on their content, behavior, and contextual information. Deep learning models, often utilizing neural networks, are capable of processing message content and behavior to learn normal patterns and differentiate them from malicious ones [41]–[44]. This real-time intrusion detection capability is vital for preventing unauthorized access and potential threats.

Case study: consider a connected vehicle network equipped with a deep learning-based intrusion detection system. In this scenario, the system successfully identifies a malicious message attempting to inject false traffic information. It promptly blocks the message and alerts nearby vehicles, effectively preventing the spread of misinformation.

4.3. AI-Driven access control and authentication

Algorithm: vehicle identity verification with AI. The objective here is to verify the identity of vehicles and authorize their participation in V2X communications. AI-driven algorithms, incorporating cryptographic techniques, authenticate vehicles based on unique identifiers and contextual information [45]–[49]. This ensures secure access to the V2X network, mitigating the risk of unauthorized access and potential malicious interference.

Case Study: Envisioning an AI-assisted access control system within a V2X-enabled intersection, the scenario unfolds with seamless authentication and authorization of vehicles for communication within the area. Utilizing AI-driven algorithms, the system efficiently verifies the identity of vehicles, incorporating cryptographic techniques to ensure robust security measures. By validating vehicles based on unique identifiers and contextual information, the system effectively safeguards the V2X network against unauthorized access and potential malicious interference, thereby enhancing overall system integrity and reliability.

5. FUTURE DIRECTIONS

Looking towards the future of AI-driven security within the IoV realm during the transition to 6G networks, numerous promising research avenues and advancements are emerging to tackle challenges and bolster security measures. These directions encompass federated learning, explainable AI, hardware-accelerated AI, adversarial robustness, and the creation of standardized benchmarks and metrics.

Emphasizing these areas of focus holds the potential to enhance the resilience and efficacy of security protocols within the evolving landscape of 6G-enabled IoV systems.

5.1. Federated learning

Enabling collaborative training of AI models without compromising data privacy. Federated learning allows AI models to be trained across decentralized edge devices, including vehicles, without sharing raw data. This approach preserves privacy while collectively improving the security models for the entire IoV ecosystem.

5.2. Explainable AI

Developing techniques to make AI-based security decisions more transparent and understandable. Enhancing the interpretability of AI models ensures that security decisions can be understood by users, regulators, and other stakeholders. This fosters trust in the decision-making processes of AI-powered security systems.

5.3. Hardware-accelerated AI

Optimizing AI algorithms for deployment in resource-constrained IoV environments. Leveraging specialized hardware, such as accelerators and processors designed for AI workloads, enhances the efficiency of AI algorithms on edge devices and vehicles. This optimization is crucial for meeting the computational demands of real-time security applications. These future directions collectively contribute to the maturation of AI-powered IoV security in the 6G era. By fostering collaboration, improving transparency optimizing hardware utilization, ensuring resilience against attacks, and establishing standardized evaluation criteria, the security infrastructure of AI-powered IoV is set to evolve and meet the dynamic challenges of the interconnected 6G landscape.

6. OPEN RESEARCH PROBLEMS

As we navigate the evolving landscape of 6G-enabled IoV, several open research issues and challenges require the attention of researchers and practitioners in the field of AI-powered IoV security. These challenges underscore the need for further investigation to advance the state-of-the-art and ensure the secure and responsible deployment of AI technologies: i) Trade-off between security and privacy: Addressing the trade-off between robust security measures and preserving user privacy in AI-driven IoV security solutions; ii) Explainable AI in real-time: Developing explainable AI techniques that can provide real-time insights into security decisions; and iii) Secure and efficient AI for edge devices: designing secure and efficient AI algorithms for edge devices and vehicles with limited computational resources. Addressing these open research issues is essential for harnessing the full potential of AI-powered IoV security in the 6G era.

7. RESULTS

AI’s superior detection capabilities, adaptability, and privacy-preserving capabilities offer significant advantages over traditional methods. This survey analyzed the potential of AI to improve safety in connected vehicles operating on 6G networks. Our key findings highlight that AI-enhanced security in 6G-connected vehicles significantly improve safety. Compared to prior research, our approach demonstrates enhanced protection without compromising performance, paving the way for more robust IoT-based vehicular networks.

8. CONCLUSION

This comprehensive survey highlights the critical role of artificial intelligence in shaping the future of the IoV and paving the way for a safer, more resilient and connected transportation landscape. By clarifying open research questions and challenges, this study provided researchers and practitioners with a roadmap for addressing security challenges associated with AI-enabled IoV systems. Integrating AI into vehicle communication architecture represents a paradigm shift that requires a collective will to strengthen safety measures and realize the promise of connected vehicles with an unwavering commitment to reliability and safety. To achieve these goals, continued innovation and collaboration between researchers and practitioners will be paramount to foster the development of robust security systems that protect the integrity and trustworthiness of AI-based IoV ecosystems.

ACKNOWLEDGEMENT

The study is funded by the Ministry of Higher Education (MOHE) of Malaysia through the Fundamental Research Grant Scheme (FRGS) No: FRGS/1/2022//ICT06/UTEM/02/3. The authors would like to thank Universiti Teknikal Malaysia Melaka for the support

REFERENCES

[1] J. Gallego-Madrid, R. Sanchez-Iborra, J. Ortiz, and J. Santa, "The role of vehicular applications in the design of future 6G infrastructures," *ICT Express*, vol. 9, no. 4, pp. 556–570, Aug. 2023, doi: 10.1016/j.icte.2023.03.011.

[2] M. Vaezi *et al.*, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2022, doi: 10.1109/COMST.2022.3151028.

[3] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: vision and potential techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, Jul. 2019, doi: 10.1109/MNET.2019.1800418.

[4] M. A. Al-Shareeda *et al.*, "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability (Switzerland)*, vol. 14, no. 16, 2022, doi: 10.3390/su14169961.

[5] R. Ma, J. Cao, D. Feng, H. Li, X. Li, and Y. Xu, "A robust authentication scheme for remote diagnosis and maintenance in 5G V2N," *Journal of Network and Computer Applications*, vol. 198, Feb. 2022, doi: 10.1016/j.jnca.2021.103281.

[6] I. Rasheed, "Enhanced privacy preserving and truth discovery method for 5G and beyond vehicle crowd sensing systems," *Vehicular Communications*, vol. 32, Dec. 2021, doi: 10.1016/j.vehcom.2021.100395.

[7] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, Mar. 2020, doi: 10.1109/MNET.001.1900220.

[8] Z. A. Abas *et al.*, "Analytics: A review of current trends, future application and challenges," *Compusoft*, vol. 9, no. 1, pp. 3560–3565, 2020, doi: 10.6084/ijact.v9i1.986.

[9] F. Salahdine, T. Han, and N. Zhang, " Security in 5G and beyond recent advances and future challenges ," *Security and Privacy*, vol. 6, no. 1, Sep. 2023, doi: 10.1002/spy2.271.

[10] J. Miao, Z. Wang, X. Miao, and L. Xing, "A secure and efficient lightweight vehicle group authentication protocol in 5G networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–12, Sep. 2021, doi: 10.1155/2021/4079092.

[11] S. Hakak *et al.*, "Autonomous vehicles in 5G and beyond: A survey," *Vehicular Communications*, vol. 39, Feb. 2023, doi: 10.1016/j.vehcom.2022.100551.

[12] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Efficient group authentication protocol for secure 5G enabled vehicular communications," in *16th International Computer Engineering Conference, ICENCO 2020*, Dec. 2020, pp. 25–30, doi: 10.1109/ICENCO49778.2020.9357372.

[13] S. Ansari, J. Ahmad, S. A. Shah, A. K. Bashir, T. Boutaleb, and S. Sinanovic, "Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 5, Apr. 2020, doi: 10.1002/ett.3966.

[14] Hemavathi, S. R. Akhila, Y. Alotaibi, O. I. Khalaf, and S. Alghamdi, "Authentication and resource allocation strategies during handoff for 5G IoVs using deep learning," *Energies*, vol. 15, no. 6, p. 2006, Mar. 2022, doi: 10.3390/en15062006.

[15] G. Baldini, "In-vehicle network intrusion detection system using convolutional neural network and multi-scale histograms," *Information (Switzerland)*, vol. 14, no. 11, Nov. 2023, doi: 10.3390/info14110605.

[16] H. Sedjelmaci, N. Kaaniche, A. Boudguiga, and N. Ansari, "Secure attack detection framework for hierarchical 6G-enabled internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 2633–2642, Feb. 2023, doi: 10.1109/TVT.2023.3317940.

[17] H. Grover, T. Alladi, V. Chamola, D. Singh, and K. K. R. Choo, "Edge computing and deep learning enabled secure multitier network for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14787–14796, Oct. 2021, doi: 10.1109/JIOT.2021.3071362.

[18] A. Biswas and H. C. Wang, "Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain," *Sensors*, vol. 23, no. 4, Feb. 2023, doi: 10.3390/s23041963.

[19] A. Nahar, H. Sikarwar, S. Jain, and D. Das, "CacheIn: A secure distributed multi-layer mobility-assisted edge intelligence based caching for internet of vehicles," in *Proceedings-23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, CCGrid 2023*, May 2023, pp. 437–446, doi: 10.1109/CCGrid57682.2023.00048.

[20] B. Yang *et al.*, "Edge intelligence for autonomous driving in 6G wireless system: design challenges and solutions," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 40–47, Apr. 2021, doi: 10.1109/MWC.001.2000292.

[21] H. Ibn-Khedher, M. Laroui, M. Alfaqawi, A. Magnouche, H. Moungla, and H. Afifi, "6G-edge support of internet of autonomous vehicles: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1, 2024, doi: 10.1002/ett.4918.

[22] Y. Djenouri, A. Belhadi, D. Djenouri, G. Srivastava, and J. C. W. Lin, "A secure intelligent system for internet of vehicles: Case study on traffic forecasting," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 11, pp. 13218–13227, Nov. 2023, doi: 10.1109/TITS.2023.3243542.

[23] J. Yang, J. Hu, and T. Yu, "Federated AI-enabled in-vehicle network intrusion detection for internet of vehicles †," *Electronics (Switzerland)*, vol. 11, no. 22, Nov. 2022, doi: 10.3390/electronics11223658.

[24] E. S. Ali *et al.*, "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications," *Security and Communication Networks*, pp. 1–23, Mar. 2021, doi: 10.1155/2021/8868355.

[25] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, Jun. 2021, doi: 10.1109/MWC.001.2000428.

[26] T. Ojanpera, J. Scholliers, T. Sukuvaara, I. Salkari, H. Zhang, and P. Eloranta, "5G-enabled road safety and cybersecurity services for connected and automated vehicles," Apr. 2021, doi: 10.1109/VTC2021-Spring51267.2021.9448668.

[27] H. Te Wu, "The internet-of-vehicle traffic condition system developed by artificial intelligence of things," *Journal of Supercomputing*, vol. 78, no. 2, pp. 2665–2680, Jul. 2022, doi: 10.1007/s11227-021-03969-0.

[28] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: enabling technologies, challenges, and opportunities," *Proceedings of the IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022, doi: 10.1109/JPROC.2022.3173031.

[29] K. Yu, L. Lin, M. Alazab, L. Tan, and B. Gu, "Deep learning-based traffic safety solution for a mixture of autonomous and manual vehicles in a 5G-enabled intelligent transportation system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4337–4347, Jul. 2021, doi: 10.1109/TITS.2020.3042504.

[30] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjoland, and F. Tufvesson, “6G wireless systems: vision, requirements, challenges, insights, and opportunities,” in *Proceedings of the IEEE*, Jul. 2021, vol. 109, no. 7, pp. 1166–1199, doi: 10.1109/JPROC.2021.3061701.

[31] M. Alsabah *et al.*, “6G wireless communications networks: a comprehensive survey,” *IEEE Access*, vol. 9, pp. 148191–148243, 2021, doi: 10.1109/ACCESS.2021.3124812.

[32] R. Agrawal, “Comparison of different mobile wireless technology (From 0G to 6G),” *ECS Transactions*, vol. 107, no. 1, pp. 4799–4839, Apr. 2022, doi: 10.1149/10701.4799ecst.

[33] A. F. M. S. Shah, “A survey from 1G to 5G including the advent of 6G: architectures, multiple access techniques, and emerging technologies,” in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, Jan. 2022, pp. 1117–1123, doi: 10.1109/CCWC54503.2022.9720781.

[34] Y. Shi *et al.*, “Machine learning for large-scale optimization in 6G wireless networks,” *IEEE Communications Surveys and Tutorials*, vol. 25, no. 4, pp. 2088–2132, 2023, doi: 10.1109/COMST.2023.3300664.

[35] S. Wang, T. Sun, H. Yang, X. Duan, and L. Lu, “6G network: Towards a distributed and autonomous system,” Mar. 2020, doi: 10.1109/6GSUMMIT49458.2020.9083888.

[36] M. Nekovee and F. Ayaz, “Vision, enabling technologies, and scenarios for a 6G-enabled internet of verticals (6G-IoV),” *Future Internet*, vol. 15, no. 2, p. 57, Jan. 2023, doi: 10.3390/fi15020057.

[37] W. Saad, M. Bennis, and M. Chen, “A vision of 6G wireless systems: applications, trends, technologies, and open research problems,” *IEEE Network*, vol. 34, no. 3, pp. 134–142, May 2020, doi: 10.1109/MNET.001.1900287.

[38] V. L. Nguyen, P. C. Lin, B. C. Cheng, R. H. Hwang, and Y. D. Lin, “Security and privacy for 6G: A survey on prospective technologies and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.

[39] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, “The roadmap to 6G security and privacy,” *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[40] J. Huang, J. Ben Othman, S. Wang, R. Y. K. Kwok, V. C. M. Leung, and W. Sun, “Guest editorial: AI-empowered mobile edge computing in the internet of vehicles,” *IEEE Network*, vol. 35, no. 3, pp. 72–73, May 2021, doi: 10.1109/MNET.2021.9454596.

[41] 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, Jan. 2024, doi: 10.3390/s24020368.

[42] F. Tang, B. Mao, N. Kato, and G. Gui, “Comprehensive survey on machine learning in vehicular network: Technology, applications and challenges,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3, pp. 2027–2057, 2021, doi: 10.1109/COMST.2021.3089688.

[43] A. Oseni *et al.*, “An explainable deep learning framework for resilient intrusion detection in IoT-Enabled transportation networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1000–1014, Jan. 2023, doi: 10.1109/TITS.2022.3188671.

[44] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, and A. A. Ghorbani, “Security issues in internet of vehicles (IoV): a comprehensive survey,” *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100809.

[45] Y. Liu, L. Pan, and S. Chen, “A hierarchical blockchain-enabled security-threat assessment architecture for IoV,” *Digital Communications and Networks*, Feb. 2023, doi: 10.1016/j.dcan.2022.12.019.

[46] X. Deng *et al.*, “A review of 6G autonomous intelligent transportation systems: Mechanisms, applications and challenges,” *Journal of Systems Architecture*, vol. 142, Sep. 2023, doi: 10.1016/j.sysarc.2023.102929.

[47] O. Rawlley and S. Gupta, “Artificial intelligence-empowered vision-based self driver assistance system for internet of autonomous vehicles,” *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 2, Nov. 2023, doi: 10.1002/ett.4683.

[48] C. Benzaid, T. Taleb, and J. Song, “AI-based autonomic and scalable security management architecture for secure network slicing in B5G,” *IEEE Network*, vol. 36, no. 6, pp. 165–174, Nov. 2022, doi: 10.1109/MNET.104.2100495.

[49] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M. K. Mishra, and P. Lalwani, “ML-based 5G network slicing security: a comprehensive survey,” *Future Internet*, vol. 14, no. 4, p. 116, Apr. 2022, doi: 10.3390/fi14040116.

BIOGRAPHIES OF AUTHORS

Depa Ramachandraiah Kumar Raja is currently working as Post-Doctoral Researcher in the Faculty of Information and Communications Technology (FTMK) at Universiti Teknikal Malaysia, Melaka, Malaysia. He received his Bachelor of Technology (B. Tech) from JNTUA College of Engineering and Master of Technology (M. Tech) from National Institute of Technology Karnataka (NITK) Surathkal, Karnataka, India. He received a Doctor of Philosophy (Ph.D.) from St Peters University, Chennai, India for his research on an effective context-driven recommender system for e-commerce applications. His research areas include the internet of things (IoT), data mining, machine learning, and intelligent transport systems. He can be contacted at email: kumarrajadr@gmail.com.

Zuraida Abal Abas is currently an Associate Professor at the Department of Intelligent Computing and Analytics, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM). She graduated with a first-class degree in B.Sc. in Industrial Mathematics from Universiti Teknologi Malaysia (UTM), obtained M.Sc. in Operational Research from London School of Economics (LSE) and received Ph.D. in Mathematics from Universiti Teknologi Malaysia (UTM). Inspired by her interest in mathematics, operational research and analytics, she is interested in expanding her research areas in multidisciplinary fields and establishing collaborative research with other institutions and industry partners. She can be contacted at email: zuraidaa@utem.edu.my.

Chandra Sekhar Akula is a Professor and Director in Avanthi Institute of Engineering and Technology, Vizianagaram. He was awarded Ph.D. from Acharya Nagarjuna University for research on investigating drugs for PPAR gamma of diabetes mellitus. His research interests are QSAR studies, research on Diabetes Mellitus. He is the editor for Springer book on Application of Computational Intelligence to Biology. He has 20 years of administrative experience. He has published research papers in vairous journals and conferences. He is a Recipient of Best Teacher Award from JNTU Kakinada. To his credit, he has granted a patent on “Rapid plastic detection in seashore using convolutional neural networks in autonomous cleaning vehicle”. He can be contacted at email: director@aietta.ac.in.

Yellapalli Dileep Kumar is currently working as a Professor of ECE and vice principal at Sree Vidyanijethan Engineering College, Mohan Babu University Tirupati. He completed his M. Tech at JNTUK, Kakinada, and also did his Ph.D. in the field of Biomedical signal Processing at JNTUK, Kakinada. His research areas of interest include biomedical signal processing, process control and instrumentation. He has a total of 18 years of experience in teaching and research and has published more than 20 publications in the fields of biomedical, instrumentation, image processing, and signal processing. He can be contacted at email: y.dileepkumar1983@gmail.com.

Goshtu Hemanth Kumar is a distinguished professional with an extensive background in the realm of IoT. As a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), he consistently showcases remarkable expertise and unwavering commitment to his field. With a decade of experience in the education sector, he currently holds the position of Assistant Professor at REVA University, School of Electronics and Communication Engineering. His research areas include the IoT, machine learning, and intelligent transport systems. He can be contacted at email: hemanthtechi@gmail.com.

Venappagari Eswari is currently working as an Assistant Professor in the School of ECE REVA University, Bengaluru. She completed her B. Tech and M. Tech degrees from JNTUA, Anantapuram. With a keen interest in the realms of the IoT and machine learning, Eswari has accumulated six years of valuable experience in both teaching and research. She can be contacted at email: veshu115@gmail.com.