American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 05 2025
PAGE NO. 177-183

Secure, Intelligent, and Distributed Communication Architectures for Autonomous Vehicular and Robotic Systems in V2X and 6G-Era Networks

Dilnoza Zubayd qizi Ismoilova

Department of Electrical and Electronic Engineering, The University of Melbourne, Australia

Received: 01 May 2025; **Accepted:** 15 May 2025; **Published:** 31 May 2025

Abstract: The rapid convergence of autonomous systems, vehicular networks, edge intelligence, and next-generation wireless communication has fundamentally transformed the operational landscape of cyber-physical mobility ecosystems. Autonomous vehicles, cooperative robotic systems, and intelligent transportation infrastructures now rely on continuous, real-time exchange of high-volume sensor data across heterogeneous communication domains. This paradigm shift has intensified long-standing concerns related to security, privacy, latency, trust, and system resilience, particularly in Vehicle-to-Everything (V2X) environments where safety-critical decisions are made under strict temporal constraints. Against this backdrop, the present research undertakes an extensive theoretical and analytical investigation of secure communication architectures for autonomous vehicular and robotic systems, with a particular emphasis on real-time encryption, distributed intelligence, and emerging paradigms such as federated and split learning.

Building upon foundational work in secure real-time sensor data transmission for autonomous systems, recent scholarship has emphasized the necessity of encryption mechanisms that balance cryptographic robustness with computational feasibility and ultra-low latency requirements (Patil & Deshpande, 2025). However, encryption alone is insufficient in isolation. The integration of edge computing, collaborative learning frameworks, and heterogeneous V2X access technologies introduces new attack surfaces and systemic vulnerabilities that demand a holistic, multi-layered security perspective. This article synthesizes and critically evaluates existing research across vehicular networking, cybersecurity, distributed machine learning, and autonomous system safety standards, while advancing a unifying conceptual framework that aligns security mechanisms with functional safety, ethical governance, and scalability requirements in 5G- and 6G-enabled environments.

Methodologically, this study adopts a structured qualitative research design grounded in systematic literature analysis, conceptual modeling, and comparative theoretical evaluation. Rather than proposing a singular algorithmic solution, the research focuses on interpretive synthesis, identifying patterns, tensions, and gaps across diverse bodies of literature. The results articulate a set of interdependent security principles—real-time cryptographic adaptability, decentralized trust management, privacy-preserving intelligence, and lifecycle-aware system governance—that collectively define the requirements of future autonomous mobility ecosystems. The discussion extends these findings by engaging with scholarly debates on centralized versus distributed control, the trade-offs between transparency and privacy, and the implications of emerging 6G sensing and localization capabilities for security architectures.

By offering a comprehensive, theoretically grounded, and critically nuanced examination of secure communication in autonomous systems, this article contributes to the ongoing discourse on how intelligent mobility infrastructures can be designed to be not only efficient and scalable, but also trustworthy, resilient, and ethically aligned. The findings are intended to inform researchers, system architects, policymakers, and standards bodies engaged in shaping the next generation of autonomous and connected systems.

Keywords: Autonomous vehicles; V2X communication; real-time encryption; federated learning; edge computing; cybersecurity; 6G networks

INTRODUCTION

Catabolism The evolution of autonomous vehicular and robotic systems represents one of the most profound technological transformations of contemporary society, reshaping transportation, logistics, healthcare, and urban infrastructure. At the core of this transformation lies the ability of machines to perceive their environment, make decisions, and coordinate actions through continuous data exchange. Modern autonomous systems are no longer isolated entities; they are deeply embedded within networked ecosystems where vehicles, roadside infrastructure, cloud platforms, and edge devices collaboratively generate and consume sensor data in real time (Arena & Pau, 2019). This interconnectedness, while enabling unprecedented levels of efficiency and situational awareness, simultaneously exposes autonomous systems to complex security and privacy challenges that extend far beyond traditional information technology domains (Ghosal & Conti, 2020).

The emergence of Vehicle-to-Everything communication has been particularly influential in redefining the operational assumptions of intelligent transportation systems. V2X encompasses Vehicle-to-Vehicle, Vehicle-to-Infrastructure, Vehicle-to-Network, and Vehicle-to-Pedestrian interactions, each with distinct latency, reliability, and security requirements (Abboud et al., 2016). In safety-critical scenarios such as collision avoidance, cooperative lane merging, and automated platooning, communication delays or data manipulation can have immediate physical consequences. As a result, secure communication in V2X environments is not merely a matter of data confidentiality, but a prerequisite for functional safety and public trust (ISO26262, 2011).

Historically, vehicular communication security has relied on centralized public key infrastructures, certificate authorities, and predefined trust models inherited from conventional networking paradigms (Alnasser et al., 2019). While these approaches provide a baseline level of authentication and integrity, they struggle to scale effectively in highly dynamic, decentralized environments characterized by high mobility and intermittent connectivity (MacHardy et al., 2018). Moreover, the increasing reliance on real-time sensor fusion, machine learning-driven perception, and adaptive control amplifies the consequences of even subtle data integrity violations. A single compromised sensor stream can propagate erroneous information across the network, undermining collective decision-making processes (Kim et al., 2021).

Recent research has highlighted the critical role of real-time encryption mechanisms tailored specifically for autonomous systems. Unlike traditional encryption schemes designed for static data or best-effort networks, autonomous systems require cryptographic solutions that operate under strict latency constraints and limited computational budgets (Patil & Deshpande, 2025). The challenge lies in achieving an optimal balance between security strength and system responsiveness, particularly in edge-based architectures where processing resources are constrained. This tension has sparked renewed interest in lightweight cryptography, adaptive key management, and context-aware security protocols that can dynamically adjust to operational conditions (Ylianttila et al., 2020).

Simultaneously, the integration of distributed intelligence paradigms such as federated learning and split learning has introduced new dimensions to the security discourse. These approaches aim to enable collaborative model training across multiple nodes without centralized data aggregation, thereby reducing privacy risks associated with raw data sharing (McMahan et al., 2016; Vepakomma et al., 2018). In vehicular and robotic contexts, federated learning promises scalable intelligence while preserving data locality, yet it also raises concerns regarding model poisoning, inference attacks, and trustworthiness of participating nodes (Posner et al., 2021). The interplay between encrypted communication channels and privacy-preserving learning frameworks remains an open area of investigation, particularly in highly heterogeneous V2X environments.

Beyond technical considerations, the development of secure autonomous systems is increasingly influenced by regulatory, ethical, and societal factors. Standards such as SAE J3016 have formalized definitions of driving automation levels, providing a common vocabulary for discussing system capabilities and responsibilities (SAE, 2018). However, security considerations are not always explicitly aligned with these functional classifications, leading to ambiguities regarding accountability and risk allocation in partially or fully automated scenarios (Takacs et al., 2020). Furthermore, emerging discussions on ethically

aligned autonomous systems emphasize the need for transparency, explainability, and human oversight, which can sometimes conflict with security practices that prioritize opacity and data minimization (Houghtaling et al., 2024).

The advent of 5G and the conceptualization of 6G networks further complicate the security landscape. Next-generation wireless technologies promise ultra-low latency, high reliability, and integrated sensing and localization capabilities that are well suited for autonomous mobility applications (Bourdoux et al., 2020). At the same time, the increased programmability and virtualization of network functions expand the attack surface, necessitating new trust models and security assurances across the network stack (Lai et al., 2020). The convergence of communication, computation, and sensing in 6G raises fundamental questions about how security should be architected in systems where boundaries between cyber and physical domains are increasingly blurred (Ylianttila et al., 2020).

Despite the breadth of existing research, several gaps remain evident in the literature. Many studies focus narrowly on specific attack vectors or defensive mechanisms without situating them within a broader system-level context. Others emphasize either cryptographic techniques or machine learning security in isolation, overlooking the interdependencies between communication security, distributed intelligence, and functional safety. While recent contributions have begun to address real-time encryption for autonomous sensor data (Patil & Deshpande, 2025), there is a lack of comprehensive analyses that integrate these insights with emerging paradigms such as federated learning, edge computing, and 6G-enabled V2X architectures.

This article seeks to address these gaps by providing an extensive, integrative examination of secure communication architectures for autonomous vehicular and robotic systems. Rather than proposing incremental technical enhancements, the study adopts a holistic perspective that synthesizes theoretical foundations, historical developments, and contemporary scholarly debates. The central research objective is to elucidate how real-time encryption, distributed learning, and next-generation networking can be coherently aligned to support secure, scalable, and trustworthy autonomous systems. In doing so, the article aims to contribute a conceptual framework that can inform future research, system design, and policy development in the rapidly evolving domain of intelligent mobility.

Methodology

The methodological foundation of this research is rooted in a qualitative, theory-driven approach designed to accommodate the complexity and interdisciplinarity of secure autonomous systems. Given the absence of universally accepted benchmarks for evaluating holistic security architectures in V2X and autonomous robotic contexts, a purely empirical or experimental methodology would be insufficient to capture the nuanced interactions between communication protocols, cryptographic mechanisms, learning paradigms, and regulatory frameworks (Wang et al., 2019). Instead, this study employs a structured interpretive methodology that synthesizes insights from established literature, standards, and conceptual models to construct an integrative analytical narrative.

The first methodological pillar of the study is an extensive systematic literature analysis. Scholarly works spanning vehicular communication technologies, cybersecurity, distributed machine learning, edge computing, and autonomous system safety were examined to identify recurring themes, dominant assumptions, and points of contention (Ghosal & Conti, 2020; Kim et al., 2021). Particular attention was paid to studies addressing real-time constraints and safety-critical communication, as these factors are central to the operational viability of autonomous systems (Patil & Deshpande, 2025). Rather than aggregating findings through quantitative meta-analysis, the literature was analyzed through thematic coding and conceptual clustering, enabling the identification of cross-domain linkages that are often obscured in siloed research.

The second methodological component involves comparative theoretical evaluation. Competing paradigms—such as centralized versus decentralized security management, hardware-based versus software-based trust anchors, and encryption-centric versus learning-centric security strategies—were systematically compared to assess their relative strengths and limitations in autonomous contexts (Alnasser et al., 2019; Posner et al., 2021). This comparative lens facilitates a deeper understanding of trade-offs, highlighting scenarios in which certain approaches may be advantageous or problematic. For example, while centralized certificate authorities offer strong identity management, they may introduce single points of failure that are incompatible with highly dynamic vehicular networks (MacHardy et al., 2018).

A third methodological element is conceptual modeling through narrative synthesis. Instead of formal mathematical models, the study constructs descriptive system models that articulate how different security components interact across layers of the autonomous system stack. These models draw on established architectural concepts in edge computing and V2X communication, emphasizing data flows, trust boundaries, and decision-making processes (Liu et al., 2019). The choice to avoid formal modeling is intentional, as the focus of the research is on interpretive depth and conceptual integration rather than algorithmic optimization.

Methodological rigor is further reinforced through critical engagement with standards and regulatory frameworks. Documents such as ISO 26262 and SAE J3016 were analyzed to contextualize security requirements within broader notions of functional safety and automation responsibility (ISO26262, 2011; SAE, 2018). This standards-oriented perspective ensures that the analysis remains grounded in real-world deployment considerations, bridging the gap between theoretical security constructs and practical system certification processes (Takacs et al., 2020).

The limitations of this methodology are acknowledged as an integral part of the research design. The reliance on secondary sources and conceptual analysis means that the findings are inherently interpretive and may not capture emergent vulnerabilities that have yet to be documented in the literature. Additionally, the rapid pace of technological change in areas such as 6G networking and autonomous learning systems implies that some conclusions may require reevaluation as new empirical evidence emerges (Bourdoux et al., 2020). Nevertheless, the chosen methodology is well suited to the study's objective of developing a comprehensive, theoretically informed understanding of secure communication architectures in autonomous systems.

Results

The analytical synthesis of the reviewed literature reveals several interrelated findings that collectively characterize the current state and future trajectory of secure communication architectures for autonomous vehicular and robotic systems. One of the most salient results is the recognition that security in autonomous environments is inherently multi-dimensional, encompassing not only cryptographic protection but also system architecture, learning integrity, and lifecycle governance (Ghosal & Conti, 2020). This finding underscores the inadequacy of narrowly focused security solutions that address isolated threats without considering systemic interactions.

A central result concerns the critical importance of real-time encryption mechanisms tailored to the operational constraints of autonomous systems. Studies consistently emphasize that conventional encryption approaches, while robust in static or low-mobility contexts, often fail to meet the stringent latency and reliability requirements of V2X communication (Alnasser et al., 2019). The work on real-time encryption for sensor data demonstrates that adaptive cryptographic strategies—capable of dynamically adjusting key lengths, encryption modes, and processing locations—are essential for maintaining both security and performance in autonomous systems (Patil & Deshpande, 2025). This adaptability emerges as a foundational principle rather than an optional enhancement.

Another significant result relates to the role of edge computing in mediating security and intelligence. Edge-based architectures reduce communication latency and bandwidth consumption by processing data closer to its source, thereby enhancing responsiveness in safety-critical scenarios (Liu et al., 2019). However, the decentralization of computation also disperses the attack surface, increasing the need for localized trust management and secure update mechanisms. The literature on over-the-air software updates highlights that without robust authentication and integrity verification, edge nodes can become vectors for large-scale compromise (Bauwens et al., 2020). As such, edge computing simultaneously mitigates and amplifies security risks, depending on how it is integrated within the overall system architecture.

The analysis further reveals that distributed learning paradigms, particularly federated learning, are increasingly viewed as both an opportunity and a challenge for autonomous system security. By enabling collaborative model training without raw data exchange, federated learning addresses privacy concerns inherent in centralized data collection (McMahan et al., 2016). In vehicular networks, this approach aligns well with the decentralized nature of V2X environments (Posner et al., 2021). However, the results also indicate that federated learning introduces new threat vectors, including model poisoning and inference attacks, which are not fully mitigated by encrypted communication alone (Singh et al., 2019). This finding suggests that security mechanisms must extend beyond data transmission to encompass model validation and participant trust

assessment.

The comparative evaluation of communication technologies yields another notable result. While Dedicated Short-Range Communications and cellular V2X each offer distinct advantages, the literature indicates a trend toward hybrid and interoperable solutions that leverage the strengths of both approaches (Abboud et al., 2016; Bazzi et al., 2019). Security considerations play a decisive role in this convergence, as heterogeneous access technologies necessitate unified trust frameworks capable of operating across diverse network conditions. The lack of standardized security interoperability remains a persistent challenge, particularly in cross-border and multi-vendor deployment scenarios (MacHardy et al., 2018).

Finally, the results highlight an emerging alignment between security, ethics, and sustainability in autonomous systems research. Recent work on ethically aligned autonomous and robotic systems emphasizes that trustworthiness extends beyond technical robustness to include transparency, accountability, and social acceptability (Houghtaling et al., 2024). This perspective resonates with findings from robotics and sustainable development research, which argue that security architectures must be designed with long-term societal impacts in mind (Haidegger et al., 2023). Consequently, security is increasingly conceptualized as an enabler of responsible autonomy rather than a purely defensive measure.

Discussion

The findings of this study invite a deeper theoretical interpretation that situates secure communication architectures within the broader evolution of autonomous and intelligent systems. At a fundamental level, the discussion reveals a paradigm shift from perimeter-based security models toward distributed, context-aware security ecosystems. In traditional networked systems, security boundaries were relatively static, and trust could be anchored to centralized authorities (Alnasser et al., 2019). In contrast, autonomous vehicular and robotic systems operate in fluid environments where trust relationships are transient, and security decisions must be made in real time (Patil & Deshpande, 2025). This shift necessitates a reconceptualization of security as a dynamic, adaptive process embedded within system behavior.

One of the most contested issues in the literature concerns the balance between decentralization and control. Proponents of decentralized architectures argue that distributing computation, intelligence, and trust reduces single points of failure and enhances resilience against large-scale attacks (Posner et al., 2021). From this perspective, federated learning and edge-based encryption represent natural extensions of the autonomous systems ethos. Critics, however, caution that excessive decentralization can undermine global situational awareness and complicate accountability, particularly in safety-critical incidents (Takacs et al., 2020). The findings of this study suggest that this debate should not be framed as a binary choice. Instead, hybrid architectures that combine localized autonomy with coordinated oversight may offer a more balanced approach, aligning security robustness with regulatory and ethical requirements.

Another key area of discussion relates to the integration of learning-based intelligence and cryptographic security. Traditionally, these domains have evolved largely independently, with cryptography focusing on data protection and machine learning emphasizing pattern recognition and decision-making (Kim et al., 2021). In autonomous systems, however, these domains intersect in complex ways. Encrypted communication channels protect sensor data in transit, but they do not inherently guarantee the integrity or fairness of learned models (Singh et al., 2019). Conversely, privacy-preserving learning techniques may reduce data exposure but still rely on secure communication infrastructures to prevent adversarial manipulation. This interdependence implies that future research must move toward co-designed security and learning frameworks rather than treating them as modular components.

The discussion also engages with the implications of emerging 6G technologies for autonomous system security. The integration of sensing, localization, and communication in 6G networks promises unprecedented levels of environmental awareness and coordination (Bourdoux et al., 2020). However, it also blurs the distinction between data sources and communication channels, potentially enabling novel attack vectors that exploit sensor spoofing or localization manipulation. From a theoretical standpoint, this convergence challenges existing security taxonomies, which often categorize threats according to discrete system layers (Ylianttila et al., 2020). A more holistic threat modeling approach, informed by cyber-physical systems theory, may be required to address these emerging risks.

Ethical and societal considerations further enrich the discussion. The literature on ethically aligned autonomous systems emphasizes that security measures must be transparent and auditable to foster public trust (Houghtaling et al., 2024). Yet transparency can conflict with security practices that rely on obscurity or proprietary mechanisms. This tension raises important questions about how to design security architectures that are both robust and explainable. The findings suggest that standardization efforts and open frameworks may play a crucial role in reconciling these objectives, enabling shared trust without compromising competitive innovation (Haidegger et al., 2023).

Limitations identified in the discussion underscore the need for continued interdisciplinary research. While the present study offers a comprehensive theoretical synthesis, empirical validation of proposed architectural principles remains an open challenge. Real-world deployments of autonomous systems are subject to contextual factors such as regulatory environments, cultural attitudes, and infrastructure maturity, which can significantly influence security outcomes (Wang et al., 2019). Future research could build on this work by conducting longitudinal case studies or large-scale simulations that examine how integrated security architectures perform under diverse operational conditions.

Conclusion

This research has undertaken an extensive, theory-driven exploration of secure communication architectures for autonomous vehicular and robotic systems operating within V2X and next-generation network environments. By synthesizing insights from cybersecurity, distributed learning, edge computing, and autonomous system standards, the study has demonstrated that security in autonomous systems is a multi-layered, dynamic construct that cannot be adequately addressed through isolated technical measures. Real-time encryption, as articulated in recent scholarship, emerges as a foundational requirement, but its effectiveness is contingent upon integration with adaptive system architectures and trust-aware intelligence frameworks (Patil & Deshpande, 2025).

The findings underscore the necessity of holistic design philosophies that align cryptographic robustness with functional safety, ethical governance, and scalability. As autonomous systems continue to proliferate across societal domains, the importance of secure, trustworthy communication infrastructures will only intensify. By advancing a comprehensive conceptual framework and engaging critically with existing scholarly debates, this article contributes to a deeper understanding of how secure autonomous systems can be responsibly developed and deployed in an increasingly connected world.

References

1. Arena, F., & Pau, G. (2019). An overview of vehicular communications. Future Internet, 11, 27.

2. Patil, A. A., & Deshpande, S. (2025). Real-time encryption and secure communication for sensor data in autonomous systems. Journal of Information Systems Engineering and Management, 10(415), 41–55.

3. Haidegger, T., Mai, V., Mörch, C., Boesl, D., Jacobs, A., Rao, B. R., Khamis, A., Lach, L., & Vanderborght, B. (2023). Robotics: Enabler and inhibitor of the Sustainable Development Goals. Sustainable Production and Consumption, 43, 422–434.

4. Abboud, K., Omar, H. A., & Zhuang, W. (2016). Interworking of DSRC and cellular network technologies for V2X communications: A survey. IEEE Transactions on Vehicular Technology, 65, 9457–9470.

5. McMahan, H. B., Moore, E., Ramage, D., & y Arcas, B. A. (2016). Federated learning of deep networks using model averaging. arXiv preprint arXiv:1602.05629.

6. Bauwens, J., Ruckebusch, P., Giannoulis, S., Moerman, I., & De Poorter, E. (2020). Over-the-air software updates in the Internet of Things: An overview of key principles. IEEE Communications Magazine, 58(2), 35–41.

7. Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A survey. Computer Networks, 169, 107093.

8. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Röning, J. (2020). 6G white paper: Research challenges for trust, security and privacy. arXiv preprint arXiv:2004.11665.

9. Posner, J., Tseng, L., Aloqaily, M., & Jararweh, Y. (2021). Federated learning in vehicular networks: Opportunities and solutions. IEEE Network, 35(2), 152–159.

10. Kim, K., Kim, J. S., Jeong, S., Park, J. H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & Security, 102150.

11. Liu, S., et al. (2019). Edge computing for autonomous driving: Opportunities and challenges. Proceedings of the IEEE, 107(8), 1697–1716.

12. Bourdoux, A., Barreto, A. N., van Liempd, B., de Lima, C., Dardari, D., Belot, D., & Suutala, J. (2020). 6G white paper on localization and sensing. arXiv preprint arXiv:2006.01779.

13. Houghtaling, M. A., Fiorini, S. R., Fabiano, N., Gonçalves, P. J., Ulgen, O., Haidegger, T., Carbonera, J. L., Olszewska, J. I., Page, B., & Murahwi, Z. (2024). Standardizing an ontology for ethically aligned robotic and autonomous systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54, 1791–1804.

14. MacHardy, Z., Khan, A., Obana, K., & Iwashina, S. (2018). V2X access technologies: Regulation, research, and remaining challenges. IEEE Communications Surveys & Tutorials, 20, 1858–1877.

15. ISO. (2011). ISO 26262: Road vehicles—Functional safety. Geneva: International Organization for Standardization.

16. SAE International. (2018). Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles (J3016).

17. Bazzi, A., Cecchini, G., Menarini, M., Masini, B. M., & Zanella, A. (2019). Survey and perspectives of vehicular Wi-Fi versus sidelink cellular-V2X in the 5G era. Future Internet, 11, 122.

18. Takacs, A., Drexler, D. A., Galambos, P., Rudas, I. J., Haidegger, T., & Csizmadia, T. (2020). Automotive safety in the development pipeline of highly automated vehicles. IEEE Systems, Man, and Cybernetics Magazine, 6, 35–40.

19. Singh, A., et al. (2019). Detailed comparison of communication efficiency of split learning and federated learning. arXiv preprint arXiv:1909.09145.

20. Wang, J., Shao, Y., Ge, Y., & Yu, R. (2019). A survey of vehicle to everything (V2X) testing. Sensors, 19, 334.