



A Novel Authentication Systems in Vehicular Communication: Challenges and Future Directions

Vugar Abdullayev^{1,2} , Alex Khang³ , Nazila Ragimova,¹ , Mohammed Almaayah⁴ 

¹ Department of Computer Engineering, Azerbaijan State Oil and Industry University, Baku, Azerbaijan, Azerbaijan

² Department of Information Technology and Systems, Azerbaijan University of Architecture and Construction

³ Global Research Institute of Technology and Engineering, Raleigh, United States

⁴ Fellowship Researcher, INTI International University, Nilai 71800, Malaysia

ARTICLE INFO

Received: 05-04-2025
Revised: 14-08-2025
Accepted: 20-08-2025
Published: 21-08-2025

Vol.2025, No.3

DOI:

<https://doi.org/10.63180/jcsra.thestap.2025.3.9>

*Corresponding author.

Email:

abdulvugar@mail.ru

Orcid:

<https://orcid.org/0000-0002-3348-2267>

This is an open access article under the CC BY 4.0 license

(<http://creativecommons.org/licenses/by/4.0/>).

Published by STAP Publisher.

ABSTRACT

The emergence of intelligent transportation systems and the widespread deployment of connected and autonomous vehicles (CAVs) have introduced unprecedented security demands in vehicular communication networks. Authentication, as a foundational security service, ensures trust among vehicles, infrastructure, and external entities. However, traditional methods such as Public Key Infrastructure (PKI) often fail to meet the stringent requirements of vehicular environments, including real-time responsiveness, scalability, and user privacy. This paper presents a comprehensive review of novel authentication systems designed for vehicular communication. We classify and analyze state-of-the-art approaches including lightweight cryptographic protocols, group-based schemes, blockchain-integrated authentication, AI-driven behavioral methods, pseudonym-based privacy-preserving mechanisms, and post-quantum cryptographic frameworks. Each system is evaluated in terms of latency, privacy, scalability, real-time capability, and maturity level. We further identify key challenges such as certificate revocation, interoperability, and ethical implications. Finally, the paper highlights emerging research directions including federated authentication, quantum-safe security, context-aware mechanisms, and hybrid blockchain-AI solutions. Our analysis serves as a roadmap for researchers and practitioners aiming to develop secure, efficient, and scalable authentication systems for next-generation vehicular networks.

Keywords: Vehicular communication, V2X security, authentication systems, blockchain, AI-based authentication, pseudonym schemes, post-quantum cryptography, intelligent transportation systems, privacy preservation, federated learning, real-time security.

How to cite the article

Abdullayev, V., Khang, A., Ragimova, N., & Almaayah, M. (2025). A Novel Authentication Systems in Vehicular Communication: Challenges and Future Directions. Journal of Cyber Security and Risk Auditing, 2025(3), 123–135. <https://doi.org/10.63180/jcsra.thestap.2025.3.9>



1. Introduction

The rapid evolution of intelligent transportation systems (ITS) and the proliferation of connected and autonomous vehicles (CAVs) have transformed the landscape of vehicular communication [1–3]. Modern vehicles now interact not only with each other (V2V) but also with infrastructure (V2I), pedestrians (V2P), and broader networks (V2X), enabling real-time data exchange to enhance road safety, traffic efficiency, and user experience[4, 5].

However, this increased connectivity brings with it significant security challenges. Authentication — the process of verifying the identity of entities involved in communication — is one of the most fundamental security services in vehicular networks [6]. Traditional authentication mechanisms, such as Public Key Infrastructure (PKI), have served as the backbone of vehicular security architectures [7, 8]. Yet, they often fall short in meeting the demanding requirements of V2X systems, which include ultra-low latency, high scalability, robust privacy, and dynamic trust management [9, 10].

To address these challenges, researchers have proposed a range of novel authentication systems. These include lightweight cryptographic techniques, group-based authentication, AI and machine learning-based behavioral systems, pseudonym and privacy-preserving protocols, blockchain-driven decentralized identity management, and emerging post-quantum cryptographic schemes. While promising, these approaches bring new complexities related to interoperability, computational cost, and privacy trade-offs.

This review paper aims to systematically explore and compare these novel authentication systems in the context of vehicular communication. We provide a comprehensive classification of existing methods, analyze their performance and limitations, and highlight unresolved challenges. Furthermore, we propose future research directions to guide the development of next-generation secure authentication mechanisms that are aligned with the evolving needs of vehicular networks.

The rest of the paper is structured as follows: Section 2 presents a classification of authentication systems. Section 3 focuses on novel mechanisms tailored for vehicular environments. Section 4 offers a comparative analysis across key evaluation metrics. Section 5 outlines critical challenges. Section 6 discusses future research directions, and Section 7 concludes the paper.

2. Classification of Authentication Systems

Authentication in vehicular communication is essential to ensure the reliability and integrity of messages exchanged between vehicles (V2V), with infrastructure (V2I), and broader networks (V2X). This section classifies authentication systems used in vehicular networks, outlining their principles, advantages, and limitations.

2.1 PKI-Based Authentication Systems

Public Key Infrastructure (PKI) is a well-established method in vehicular networks. Each vehicle is issued a digital certificate by a trusted Certificate Authority (CA), enabling message signing and verification through public-private key pairs [11, 12]. PKI-based systems provide strong cryptographic guarantees for authenticity and message integrity [13–15]. They are well-standardized and have been adopted in frameworks like IEEE 1609.2, making them widely deployable and trustworthy [16–20]. These systems suffer from high overhead in certificate revocation and renewal, particularly in highly dynamic environments. They also offer limited privacy since vehicle identities can be traced via certificates, and a compromised CA could potentially disrupt the entire system [5, 21, and 22].

2.2 Group-Based Authentication

Group-based authentication involves authenticating vehicles as members of a logical group using shared keys or group signatures. This approach reduces the need to authenticate each vehicle individually [23–26]. It offers significant improvements in efficiency and scalability, especially in dense vehicular environments, by minimizing cryptographic operations for individual vehicles within the same group [27–29]. Managing group keys and ensuring secure re-keying after member changes can be complex [30, 31]. Moreover, compromised vehicles within the group can pose internal threats that are harder to isolate [32–34].

2.3 Blockchain-Based Authentication

Blockchain technology enables decentralized identity verification and trust establishment through distributed ledgers and smart contracts. Blockchain eliminates the need for a centralized authority, providing a tamper-proof, transparent, and auditable authentication mechanism [35–39]. This is particularly beneficial for building long-term trust and secure identity management in vehicular networks. Despite its benefits, blockchain introduces latency and computational burdens that make it unsuitable for real-time vehicular communications. Additionally, scalability remains a concern as the number of vehicles and transactions increases.

2.4 AI/ML-Based Behavioral Authentication

Machine learning approaches authenticate vehicles based on behavioral data such as driving style, speed, and trajectory, enabling more dynamic and adaptive verification. These systems enable continuous and context-aware authentication, improving security without requiring explicit user input [40–44]. They are effective in detecting anomalies or spoofed behaviors that traditional methods might miss. Their performance heavily depends on the availability of large, diverse training datasets. They can also be affected by legitimate changes in behavior (e.g., different drivers), leading to false positives or reduced accuracy.

2.5 Pseudonym-Based and Privacy-Preserving Authentication

This category involves frequently changing pseudonyms and privacy techniques to prevent vehicle tracking and identity exposure [45–51]. By obfuscating vehicle identities through pseudonyms and mix-zones, these systems offer a high degree of privacy protection while maintaining authentication validity [52–54]. They are also compatible with most existing V2X infrastructures [55–59]. Pseudonym management requires secure synchronization and timely updates. If these mechanisms fail or are compromised, the vehicle's privacy can be exposed or even exploited [60, 61].

2.6 Post-Quantum Cryptography-Based Authentication

With quantum computing on the horizon, researchers are exploring post-quantum cryptographic techniques for long-term security. These schemes promise resilience against quantum-enabled attacks, offering future-proof authentication methods crucial for the longevity of vehicular systems deployed today [62, 63, 63, 64]. Post-quantum algorithms are currently computationally expensive and often unsuitable for real-time or resource-constrained environments. Their integration into vehicular systems is still in early experimental stages.

3. Comparative Analysis of Novel Systems

To evaluate the practical applicability and effectiveness of various novel authentication systems in vehicular environments, it is essential to analyze their performance across key criteria. This section compares these systems based on latency, privacy, scalability, real-time capability, and maturity level.

3.1 Evaluation Criteria

- Latency: Authentication delay, with lower latency preferred in real-time vehicular scenarios.
- Privacy: Protection of vehicle identity and location information from tracking or Inference.
- Scalability: The system's ability to handle large numbers of nodes and high message frequency.
- Real-Time Capability: Suitability for instantaneous decision-making in safety-critical contexts.
- Maturity: Degree of technological readiness and deployment in real-world systems.

3.2 System Comparison Overview

To provide a comparative overview of the discussed authentication methods in vehicular networks, Table 1 summarizes their key characteristics in terms of latency, privacy, scalability, real-time capability, and maturity. This comparison highlights the trade-offs between different approaches and helps identify the most suitable techniques for specific vehicular scenarios such as high-speed V2V communication or privacy-sensitive V2X environments.

Table 1. Comparison of Authentication Methods in Vehicular Networks

| Method | Latency | Privacy | Scalability | Real-time | Maturity |
|------------------------|---------|---------|-------------|-----------|--------------|
| PKI-Based | Medium | Low | Medium | Yes | High |
| Group-Based | Low | Medium | High | Yes | Moderate |
| Blockchain-Based | High | High | Medium | No | Low |
| AI/ML | Low | Medium | Medium | Yes | Experimental |
| Behavioral | | | | | |
| Pseudonym-Based | Low | High | High | Yes | High |
| Post-Quantum Crypto | High | Medium | Low | No | Low |

3.3 Insights and Observations

Pseudonym-based authentication systems emerge as the most balanced approach, combining strong privacy, scalability, and real-time performance. Their high maturity level further supports their deployment in current V2X networks. Figure 1 depicts the Pseudonym-based approach. It performs strongly across all criteria, especially in privacy and scalability, making it a mature and practical solution for V2X applications.

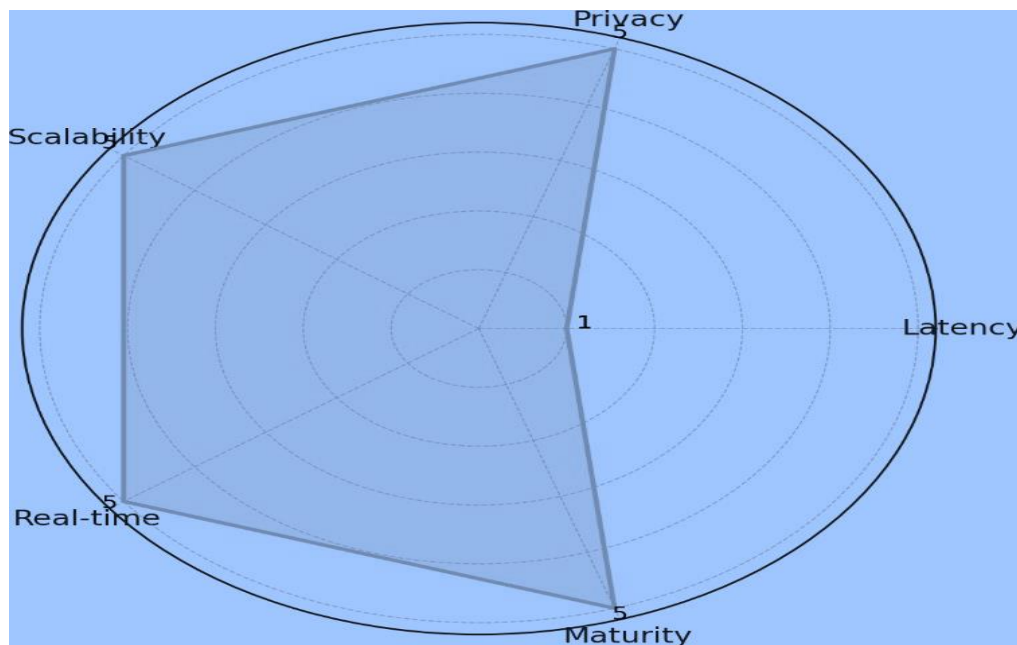


Figure 1. Evaluation on Pseudonym-Based and Privacy-Preserving Authentication Systems

Group-based systems are ideal for high-density environments due to their efficiency, although improvements in trust management are necessary. Figure 2 presents the Group-based authentication scheme. It achieves high scalability and low latency, making it suitable for dense environments, though it scores moderately on privacy and maturity. Blockchain-based methods, while highly privacy-preserving and decentralized, currently lack real-time suitability and need advancements in latency reduction and network scalability. Figure 3 displays the Blockchain-based method, which offers high privacy but suffers from high latency and lower real-time suitability, limiting its current use in time-critical vehicular scenarios. AI/ML-based behavioral systems offer context-aware, adaptive authentication but remain experimental. Key challenges include model generalization, training data availability, and explainability. Figure 4 shows the AI/ML-based behavioral authentication system. It excels in real-time adaptability and latency but remains experimental with moderate scalability and privacy. Post-quantum cryptographic systems are critical for future-proofing authentication but are not yet suitable for real-time vehicular applications due to computational complexity. Figure 5 visualizes the Post-Quantum Cryptography-based method.

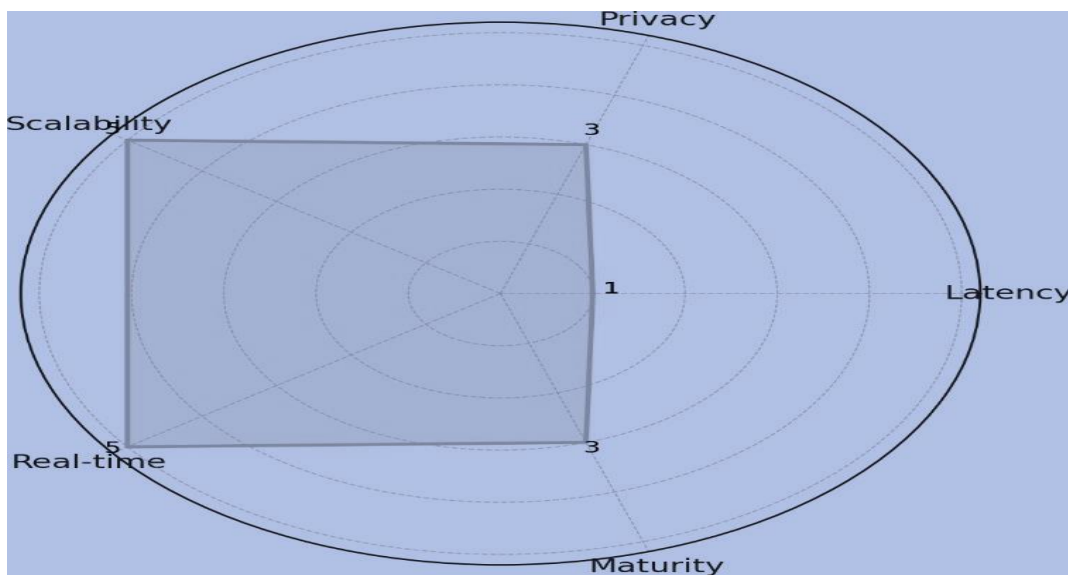


Figure 2. Evaluation on Group-Based Authentication Systems

Although promising in future-proof security, its current limitations in latency, scalability, and real-time performance are evident. Traditional PKI systems are mature and reliable but underperform in privacy and revocation speed, highlighting the need for more privacy-aware enhancements. Figure 6 illustrates the performance of the PKI-based authentication system. It shows balanced maturity and real-time capability, but moderate scalability and low privacy due to certificate traceability concerns.

4. Key Challenges

Despite significant advances in authentication mechanisms for vehicular networks, a number of challenges remain that hinder their seamless deployment in real-world intelligent transportation systems. These challenges span across technical, operational, and regulatory domains and must be addressed to ensure secure, scalable, and privacy-preserving communication.

4.1 Real-Time Constraints

Vehicular communication environments are characterized by high mobility and stringent latency requirements. Authentication schemes must be extremely efficient to meet the sub-second response times required by safety-critical

applications such as Collision avoidance and emergency braking. Traditional cryptographic operations, certificate validation, and blockchain consensus protocols often introduce delays that are unacceptable for real-time systems.

4.2 Scalability in Dense Networks

Urban environments with high vehicle densities pose scalability issues for many authentication schemes. For instance, broadcast authentication in group-based systems or blockchain synchronization can become bottlenecks. The challenge lies in maintaining low latency and high throughput while supporting thousands of simultaneous authentication requests in real-time.

4.3 Privacy vs. Traceability

There is an inherent tension between privacy preservation and accountability in vehicular networks. While vehicles require anonymity to prevent tracking and profiling, regulatory authorities must retain the ability to trace misbehaving nodes when necessary. Achieving conditional privacy — where anonymity is preserved under normal operation but revocable in the case of misuse — remains an unsolved problem.

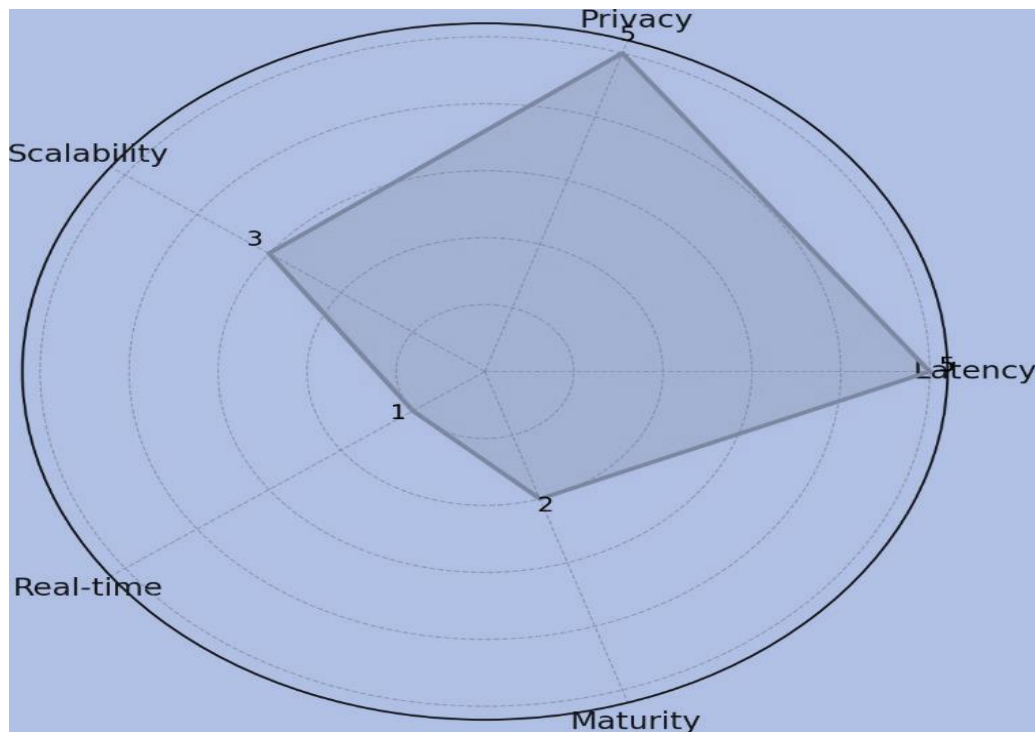


Figure 3. Evaluation on Blockchain-Based Authentication Systems

4.4 Certificate and Key Revocation

Effective revocation of compromised credentials is a major challenge, particularly in PKI-based systems. The distribution of Certificate Revocation Lists (CRLs) or the real-time querying of revocation status introduces communication and computation overhead. Delayed revocation can allow malicious vehicles to remain trusted within the network, undermining security.

4.5 Interoperability and Standardization

The lack of unified standards across different regions and manufacturers complicates the implementation of authentication protocols. For example, Europe and the US have different vehicular communication stacks (C-ITS vs DSRC). Furthermore, proprietary solutions may not interoperate seamlessly, creating fragmented trust boundaries and vulnerabilities in cross-border vehicular scenarios.

4.6 Security against Advanced Attacks

Emerging authentication systems must defend against sophisticated adversarial techniques including Sybil attacks, relay attacks, GPS spoofing, and machine learning-based impersonation. AI-enhanced attackers may attempt to mimic behavioral authentication profiles, while blockchain-based systems may face smart contract exploits or 51% attacks. Developing resilient mechanisms that can anticipate and adapt to evolving threats is essential.

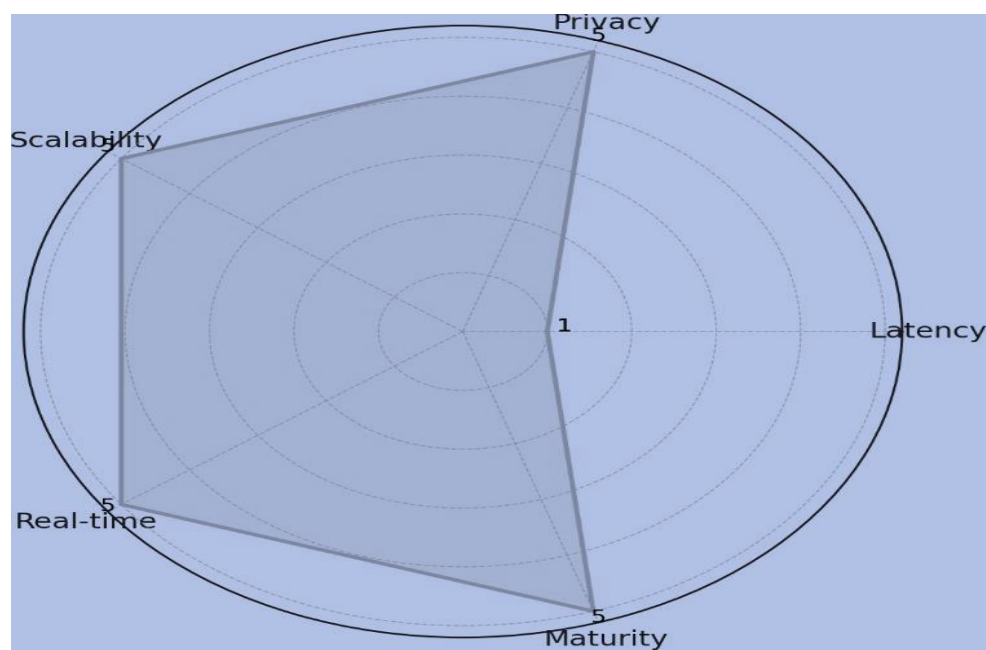


Figure 5. Evaluation on Post-Quantum Cryptography-Based Authentication Systems

4.7 Resource Constraints in On-Board Units (OBUs)

Many advanced cryptographic and AI/ML-based authentication mechanisms demand significant computation and energy resources. However, vehicular OBUs often operate under limited hardware capabilities and power budgets. Designing lightweight, efficient protocols suitable for real-time operation on constrained devices is a key technical hurdle.

4.8 Lack of Real-World Testbeds

Most proposed authentication solutions are evaluated in simulated environments or small-scale prototypes. There is a critical need for large-scale, heterogeneous, and real-world vehicular testbeds that can validate the performance, robustness, and interoperability of novel authentication protocols under realistic conditions.

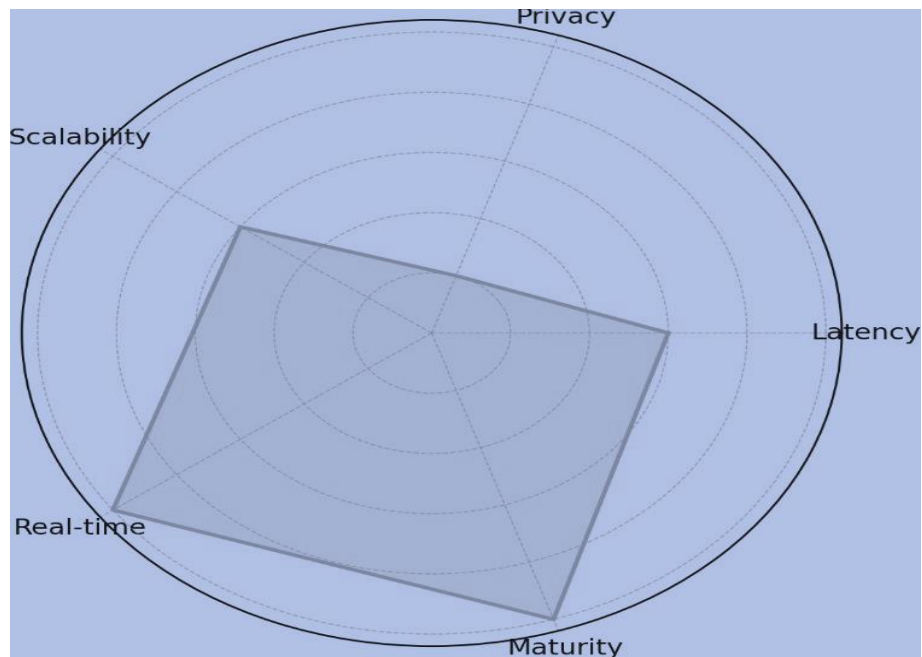


Figure. 6 Evaluation on PKI-Based Authentication Systems

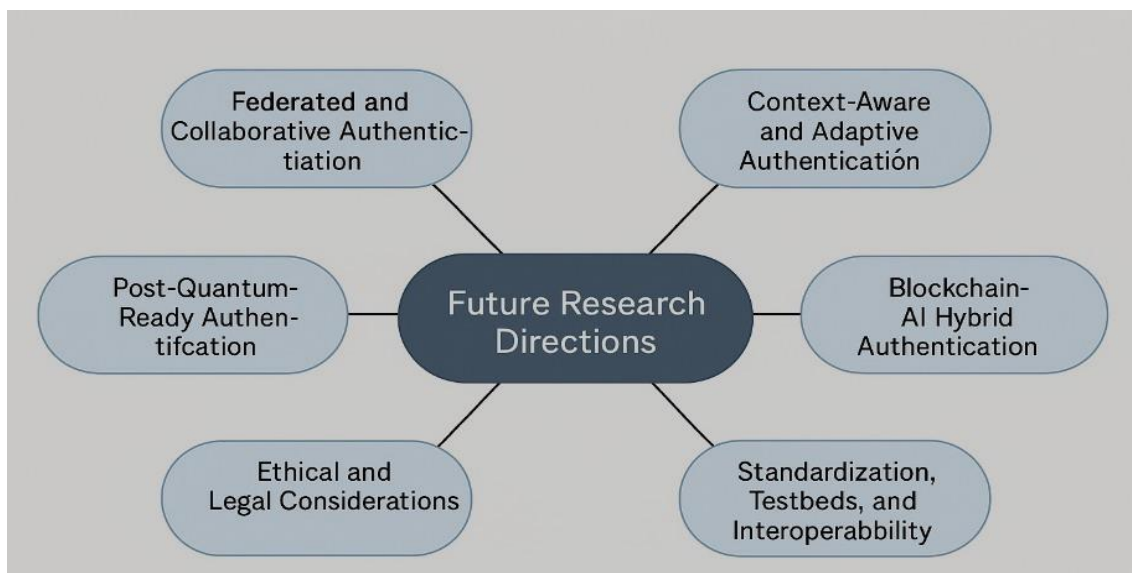


Figure 7. Future Research Directions

5. Future Research Directions

As vehicular networks transition towards highly autonomous and hyper-connected ecosystems, existing authentication mechanisms must evolve in parallel. This section outlines key research directions that address current limitations and prepare for future technological and security challenges in vehicular communication, as shown in Figure 7.

5.1 Federated and Collaborative Authentication

Federated learning allows vehicles and infrastructure units to collaboratively train authentication models without sharing raw data. This decentralized approach enhances privacy and scalability. Future research should explore federated behavioral biometrics, privacy-preserving model updates, and defenses against poisoning or inversion attacks in vehicular contexts.

5.2 Post-Quantum-Ready Authentication

Quantum computing poses a threat to current cryptographic primitives. Research is needed to develop lightweight post-quantum cryptography (PQC) schemes that are compatible with the computational constraints of on-board vehicular units. Priority areas include integrating lattice-based and hash-based algorithms into V2X authentication protocols and evaluating their real-time performance.

5.3 Context-Aware and Adaptive Authentication

Authentication systems must adapt dynamically to vehicular context, including speed, location, and environmental conditions. This ensures security without compromising system responsiveness. Future systems should implement real-time scoring models, dynamic threshold adjustment, and multimodal data fusion using sensor, biometric, and behavioral inputs.

5.4 Blockchain-AI Hybrid Authentication

Combining blockchain's decentralization and immutability with AI's pattern recognition capabilities offers a robust authentication paradigm. AI can detect anomalies, while blockchain ensures verifiability. Research should focus on blockchain-secured behavioral profiles, smart contract-based access control, and lightweight distributed ledgers suitable for low-latency vehicular environments.

5.5 Seamless Authentication in 5G/6G-Enabled V2X

Emerging 5G and 6G networks provide ultra-low latency and massive connectivity, necessitating scalable and fast authentication mechanisms. Key areas include edge-assisted authentication using network slicing, secure handover protocols in high-mobility scenarios, and context-driven trust frameworks for multi-access edge computing (MEC) environments.

5.6 Standardization, Testbeds, and Interoperability

Despite technical advancements, deployment remains limited due to lack of standardized frameworks and interoperable platforms. There is a pressing need for international cooperation. Future work should prioritize open-source testbeds, harmonized security standards (e.g., SCMS, C-ITS, C-V2X), and certification schemes for novel authentication solutions.

5.7 Ethical and Legal Considerations

With the increased use of biometric and behavioral data, ethical and legal aspects become critical. These include privacy, consent, and ownership of driver data. Researchers must consider compliance with regulations like GDPR and explore ethical frameworks for continuous surveillance, driver profiling, and AI-based scoring systems.

6. Conclusion

Vehicular communication networks are rapidly transforming with the rise of intelligent transportation systems, autonomous driving, and pervasive connectivity. In this dynamic context, robust, low-latency, and privacy-preserving authentication mechanisms are essential to ensure secure and trustworthy communication among vehicles and between vehicles and infrastructure. This review has presented a comprehensive classification of both traditional and novel authentication systems, highlighting their underlying principles, strengths, and limitations. Novel systems such as AI-driven behavioral authentication, blockchain-based identities, group signatures, pseudonym-based methods, and post-quantum cryptographic

schemes represent promising directions that address the unique challenges of vehicular environments, including real-time performance, privacy concerns, and scalability. The comparative analysis demonstrated that no single solution meets all performance criteria, underscoring the necessity for hybrid models that combine multiple techniques to balance latency, privacy, and robustness. Moreover, current limitations in revocation handling, interoperability, and legal compliance remain key barriers to widespread adoption. Looking ahead, future research should focus on federated authentication, quantum-safe mechanisms, and AI-integrated frameworks that adapt to vehicular contexts in real time. Standardization efforts, real-world testbeds, and regulatory harmonization will also be critical to transition these technologies from research prototypes to deployment-ready systems.

In conclusion, authentication in vehicular communication remains a vibrant and evolving field, central to the success of future smart mobility and secure transportation infrastructures. Collaborative efforts across disciplines—spanning cryptography, artificial intelligence, network engineering, and legal policy—will be essential to realize secure, scalable, and privacy-aware vehicular networks.

Corresponding author

Vugar Abdullayev
abdulvugar@mail.ru

Acknowledgements

Not applicable.

Funding

No funding.

Contributions

V.A.; A.K.; N.R.; M.A.; Conceptualization, V.A.; A.K.; N.R.; M.A.; Investigation, V.A.; A.K.; N.R.; M.A.; Writing (Original Draft), V.A.; A.K.; N.R.; M.A.; Writing (Review and Editing) Supervision, V.A.; A.K.; N.R.; M.A. Project Administration.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Competing interests

All authors declare no competing interests.

References

- [1] Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2024). Software defined networking for internet of things: Review, techniques, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics*.
- [2] Al-Mekhlafi, Z. G., Lashari, S. A., Al-Shareeda, M. A., Mohammed, B. A., Alshudukhi, J. S., Al-Dhlan, K. A., & Manickam, S. (2024). Coherent taxonomy of vehicular ad hoc networks (VANETs) enabled by fog computing: A review. *IEEE Sensors Journal*, 24, 29575–29602.
- [3] Mohammed, B. A., Al-Shareeda, M. A., Alsadhan, A. A., Al-Mekhlafi, Z. G., Sallam, A. A., Al-Qatab, B. A., Alshammari, M. T., & Alayba, A. M. (2024). Service based veins framework for vehicular ad-hoc network (VANET): A systematic review of state-of-the-art. *Peer-to-Peer Networking and Applications*, 17, 2259–2281.
- [4] Al-Shareeda, M. A., & Manickam, S. (2023). A systematic literature review on security of vehicular ad-hoc network (VANET) based on veins framework. *IEEE Access*, 11, 46218–46228.
- [5] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. *International Journal of Engineering and Management Research*.
- [6] Almansor, M. J., Din, N. M., Baharuddin, M. Z., Alsayednoor, H. M., Al-Shareeda, M. A., Ma, M., & Al-asadi, A. J. (2025). Vessel berthing system using internet of things (IoT) for smart port. *AIP Conference Proceedings*.
- [7] Al-Shareeda, M. A., Yue, L., & Manickam, S. (2024). Review of edge computing for the internet of things (EC-IoT): Techniques, challenges and future directions. *Journal of Sensor Networks and Data Communications*.

- [8] Al-Shareeda, M. A., Alazzawi, M. A., Anbar, M., Manickam, S., & Al-Ani, A. K. (2021). A comprehensive survey on vehicular ad hoc networks (VANETs). In *2021 International Conference on Advanced Computer Applications (ACA)* (pp. 156–160).
- [9] Al-Shareeda, M. A., Manickam, S., & Sari, S. A. (2022). A survey of SQL injection attacks, their methods, and prevention techniques. In *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)* (pp. 31–35).
- [10] Olumide, M. L., Habib, A. M. M., Halim, F. A., Vijayan, G. A., Rusly, N. S., Fadzil, L. M., Al-Shareeda, M. A., & Manickam, S. (2023). Proposed order management system (OMS) for Gazi Communications. *Journal of Computer Science & Computational Mathematics*.
- [11] Arfeen Laghari, S., Manickam, S., Al-Ani, A. K. I., Al-Shareeda, M. A., & Karuppayah, S. (2023). ES-SECS/GEM: An efficient security mechanism for SECS/GEM communications. *IEEE Access*, *11*, 31813–31828.
- [12] Almansor, M. J., Din, N. M., Baharuddin, M. Z., Ma, M. D., Alsayednoor, H. M., Al-Shareeda, M. A., & Al-Asadi, A. J. (2024). Routing protocols strategies for flying ad-hoc network (FANET): Review, taxonomy, and open research issues. *Alexandria Engineering Journal*.
- [13] Al-Shareeda, M. A., Anbar, M., Alazzawi, M. A., Manickam, S., & Al-Hiti, A. S. (2020). LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access*, *8*, 170507–170518.
- [14] Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2023). Long range technology for internet of things: Review, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics*.
- [15] Al-Shareeda, M. A., Manickam, S., Arfeen Laghari, S., & Jaisan, A. (2022). Replay-attack detection and prevention mechanism in Industry 4.0 landscape for secure SECS/GEM communications. *Sustainability*.
- [16] Hamdi, M. M., Audah, L. M., Rashid, S. A., & Shareeda, M. A. (2020). Techniques of early incident detection and traffic monitoring centre in VANETs: A review. *Journal of Communications*, *15*, 896–904.
- [17] Shareeda, M. A., Khalil, A., & Fahs, W. (2019). Realistic heterogeneous genetic-based RSU placement solution for V2I networks. *International Arab Journal of Information Technology*, *16*, 540–547.
- [18] Hamdi, M. M., Mustafa, A. S., Mahd, H. F., Abood, M. S., Kumar, C., & Al-Shareeda, M. A. (2020). Performance analysis of QoS in MANET based on IEEE 802.11b. In *2020 IEEE International Conference for Innovation in Technology (INOCON)* (pp. 1–5).
- [19] Hou, P. S., Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). Vector autoregression model-based forecasting of reference evapotranspiration in Malaysia. *Sustainability*.
- [20] Zijie, F., Al-Shareeda, M. A., Saare, M. A., Manickam, S., & Karuppayah, S. (2023). Wireless sensor networks in the internet of things: Review, techniques, challenges, and future directions. *Indonesian Journal of Electrical Engineering and Computer Science*.
- [21] Shukla, V., Al-Shareeda, M. A., Dixit, S., & Gupta, S. (2025). A secure audio transmission method. In *International Conference on Emerging Trends in Artificial Intelligence, Data Science and Signal Processing* (pp. 141–155). Springer.
- [22] Shareeda, M. A. A., & Manickam, S. (2022). Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. *Symmetry*, *14*, 1543.
- [23] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). Enhancement of NTSA secure communication with one-time pad (OTP) in IoT. *Informatica (Slovenia)*, *47*.
- [24] Hwa, K. C., Manickam, S., & Al-Shareeda, M. A. (2022). Review of peer-to-peer botnets and detection mechanisms. *ArXiv*, abs/2207.12937.
- [25] Al-Shareeda, M. A., Saare, M. A., Manickam, S., & Karuppayah, S. (2023). Validation of the toolkit for fake news awareness in social media. *Indonesian Journal of Electrical Engineering and Computer Science*.
- [26] Abdullahi, A., Manickam, S., Karuppayah, S., & Al-Shareeda, M. A. (2023). Proposed enhanced link failure rerouting mechanism for software-defined exchange point. *Indonesian Journal of Electrical Engineering and Computer Science*.
- [27] Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). A review of an emerging cyber kill chain threat model. In *2023 Second International Conference on Advanced Computer Applications (ACA)* (pp. 157–161).
- [28] Shen, W. Y., Manickam, S., & Al-Shareeda, M. A. (2022). A brief review of advanced monitoring mechanisms in peer-to-peer (P2P) botnets. In *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)* (pp. 312–317).
- [29] Al-Hiti, A. S., Sahbudin, R. K. Z., Harun, S. W., Obaid, A. N., Hamdi, M. M., & Al-Shareeda, M. A. (2023). Wireless body area networks: Applications and congestion control technologies. In *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1–7).
- [30] Alomari, M. Q. M., & Alshwaikh, F. J. A. (2023). The network security (NS) of healthcare and medical facilities: An analytical overview of the emerging cybersecurity threats/risks and countermeasures. *International Journal of Advanced Research*.
- [31] Al-Shareeda, M. A., Manickam, S., Saare, M. A., Sari, S. A., & Alazzawi, M. A. (2022). Controlling COVID-19 with Internet of Things (IoT) technologies: A review. In *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)* (pp. 6–11).
- [32] Al-Shareeda, M. A., Manickam, S., Saare, M. A., Karuppayah, S., & Alazzawi, M. A. (2022). Detection mechanisms for peer-to-peer botnets: A comparative study. In *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)* (pp. 267–272).
- [33] Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in health IoT. *Sensors (Basel, Switzerland)*, *23*.
- [34] Wu, C. C., Ahmad, S. A., Fadzil, L. M., Ishak, M. K., Manickam, S., & Al-Shareeda, M. A. (2023). Proposed smart water management system. In *2023 Second International Conference on Advanced Computer Applications (ACA)* (pp. 1–4).
- [35] Almazroi, A. A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024). FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet of Things*, *25*, 101096.

- [36] Mohammed, B. A., Al-Shareeda, M. A., Al-Mekhlafi, Z. G., Alshudukhi, J. S., & Al-Dhlan, K. A. (2024). HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks. *IEEE Access*, *12*, 6251–6261.
- [37] Mohammed, B. A., Al-Shareeda, M. A., Alsadhan, A. A., Al-Mekhlafi, Z. G., Sallam, A. A., Al-Qatab, B. A., Alshammari, M. T., & Alayba, A. M. (2024). Efficient blockchain-based pseudonym authentication scheme supporting revocation for 5G-assisted vehicular fog computing. *IEEE Access*, *12*, 33089–33099.
- [38] Al-Shareeda, M. A., Saare, M. A., & Manickam, S. (2023). The blockchain internet of things: Review, opportunities, challenges, and recommendations. *Indonesian Journal of Electrical Engineering and Computer Science*.
- [39] Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Al-Shareeda, M. A., Mohammed, B. A., Alshudukhi, J. S., & Al-Dhlan, K. A. (2024). Fog computing and blockchain technology based certificateless authentication scheme in 5G-assisted vehicular communication. *Peer-to-Peer Networking and Applications*, *17*, 3703–3721.
- [40] Shammri, F. K. A., Al-Shareeda, M. A., Abbood, A. A., Almaiah, M. A., & AlAli, R. M. (2025). Quantum-enhanced AI and machine learning: Transforming predictive analytics. *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*.
- [41] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). DDoS attacks detection using machine learning and deep learning techniques: Analysis and comparison. *Bulletin of Electrical Engineering and Informatics*.
- [42] Al-Shareeda, M. A., Manickam, S., Saare, M. A., Sari, S. A., & Alazzawi, M. A. (2022). Intelligent pizza vending machine intelligence via cloud and IoT. In *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCITT)* (pp. 25–30).
- [43] Al-Shareeda, M. A., Obaid, A. A., & Almajid, A. A. H. (n.d.). The role of artificial intelligence in bodybuilding: A systematic review of applications, challenges, and future prospects.
- [44] Ahmad, W., Almaiah, M. A., Ali, A., & Al-Shareeda, M. A. (2024). Deep learning based network intrusion detection for unmanned aerial vehicle (UAV). In *2024 7th World Conference on Computing and Communication Technologies (WCCCT)* (pp. 31–36).
- [45] Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., & Manickam, S. (2021). Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sensors Journal*, *21*, 2422–2433.
- [46] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Yassin, A. A. (2020). VPPCS: VANET-based privacy-preserving communication scheme. *IEEE Access*, *8*, 150914–150928.
- [47] Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., Manickam, S., & Hanshi, S. M. (2020). Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. *IEEE Access*, *8*, 144957–144968.
- [48] Al-Shareeda, M. A., Anbar, M., Manickam, S., Khalil, A., & Hasbullah, I. H. (2021). Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. *IEEE Access*, *9*, 121522–121531.
- [49] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2021). Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access*, *9*, 113226–113238.
- [50] Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2020). An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network. *Symmetry*, *12*, 1687.
- [51] Shareeda, M. A., Manickam, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Qtaish, A., Alzahrani, A. J., Alshammari, G., Sallam, A. A., & Almekhlafi, K. (2022). CM-CPPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks. *Sensors (Basel, Switzerland)*, *22*.
- [52] Mohammed, B. A., Al-Shareeda, M. A., Manickam, S., Al-Mekhlafi, Z. G., Alreshidi, A., Alazmi, M., Alshudukhi, J. S., & Alsaffar, M. S. (2023). FC-PA: Fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks. *IEEE Access*, *11*, 18571–18581.
- [53] Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2022). A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. *Sensors (Basel, Switzerland)*, *22*.
- [54] Al-Mekhlafi, Z. G., Al-Shareeda, M. A., Manickam, S., Mohammed, B. A., Alreshidi, A., Alazmi, M., Alshudukhi, J. S., Alsaffar, M. S., & Alsewari, A. A. (2023). Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks. *Electronics*.
- [55] Shareeda, M. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2021). SE-CPPA: A secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *Sensors (Basel, Switzerland)*, *21*.
- [56] Alazzawi, M. A., Al-behadili, H. A. H., Almalki, M. N. S., Challob, A. L., & Shareeda, M. A. A. (2020). ID-PPA: Robust identity-based privacy-preserving authentication scheme for a vehicular ad-hoc network. In *International Conference on Advances in Cybersecurity*. <https://api.semanticscholar.org/CorpusID:231929822>
- [57] Al-Shareeda, M. A., Anbar, M., Alazzawi, M. A., Manickam, S., & Hasbullah, I. H. (2021). Security schemes based on conditional privacy-preserving vehicular ad hoc networks. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*, 479–488.
- [58] Al-Shareeda, M. A., Anbar, M., Manickam, S., Hasbullah, I. H., Abdullah, N., & Hamdi, M. M. (2020). NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *Applied Mathematics & Information Sciences*, *14*, 957–966.
- [59] Shareeda, M. A., Anbar, M., Manickam, S., Hasbullah, I. H., Khalil, A., Alazzawi, M. A., & Al-Hiti, A. S. (2020). Proposed efficient conditional privacy-preserving authentication scheme for V2V and V2I communications based on elliptic curve cryptography in vehicular ad hoc networks. In *International Conference on Advances in Cybersecurity*. <https://api.semanticscholar.org/CorpusID:231929886>
- [60] Almazroi, A. A. A., Alqarni, M. A., Al-Shareeda, M. A., & Manickam, S. (2023). L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system. *PLOS ONE*, *18*.

- [61] Al-Mekhlafi, Z. G., Lashari, S. A., Altmemi, J. M. H., Al-Shareeda, M. A., Mohammed, B. A., Sallam, A. A., Al-Qatab, B. A., Alshammari, M. T., & Alayba, A. M. (2024). Oblivious transfer-based authentication and privacy-preserving protocol for 5G-enabled vehicular fog computing. *IEEE Access*, *12*, 100152–100166.
- [62] Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Khalil, A., Al-Shareeda, M. A., Mohammed, B. A., Alsadhan, A. A., Alayba, A. M., Saleh, A. M. S., Al-Reshidi, H. A., & Almekhlafi, K. (2024). Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5G-assisted vehicular communications. *IEEE Access*, *12*, 71232–71247.
- [63] Abbood, A. A., Al-Shammri, F. K., Alzamili, Z., Al-Shareeda, M. A., Almaiah, M. A., & AlAli, R. M. (2025). Investigating quantum-resilient security mechanisms for flying ad-hoc networks (FANETs). *Journal of Robotics and Control (JRC)*.
- [64] Al-Mekhlafi, Z. G., Al-Shareeda, M. A., Manickam, S., Mohammed, B. A., & Qtaish, A. (2023). Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks. *Mathematics*.

Biographies



Vugar Abdullayev is a doctor of technical sciences, Assos. Prof., Azerbaijan State Oil and Industry University. Baku, Azerbaijan. He has completed his Ph.D in Computer Science in the year 2005. He is currently as a Assos. Professor of the “Computer engineering” Department at the Azerbaijan State Oil and Industry University, Baku, Azerbaijan. He is author of 155 scientific papers. His researchers related to the study of the modern information technologies, CPS, IoT, Cloud, big data and networking. abdulvugar@mail.ru



Dr. Ahmed Elkhail is a distinguished Sudanese scholar with a robust computer engineering and technology background. I completed my B.S. in 2014 and M.Sc. in 2017 at the University of Gezira, Sudan, and earned my PhD from Southwest Jiaotong University, China, in 2024. My research interests include cryptography, network security, blockchain technology, cloud computing, virtualization, and network architecture. I am an associate professor at the School of Computer and Information Engineering, Qilu Institute of Technology, China. engkhail31@qlit.edu.cn



Dr. Nazila Ragimova is a Doctor of Technical Sciences, Assoc. Prof., at the Azerbaijan State Oil and Industry University, Baku, Azerbaijan. She has been serving as the Head of the “Computer Engineering” Department since 2018. She completed her Ph.D. in Computer Science and has extensive experience in higher education and research. She is the author of more than 170 scientific publications. Her research interests include expert systems, artificial intelligence, machine learning, big data analytics, and their applications in areas such as healthcare, education, and smart systems. Ragimova.n.a@gmail.com



Dr. Mohammed Almaayah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaayah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain. m.almaayah@ju.edu.jo