STAP Journal of Security Risk Management

https://www.jsrm.thestap.com/

Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks

Aitizaz Ali [1]

[1] *School of Technology, Asia Pacific University of Technology and Innovations, Kuala Lumpur, Malaysia*

ARTICLE INFO

Article History

Received: 05-07-2024
Revised: 14-11-2024
Accepted: 15-11-2024
Published: 16-11-2024

Vol.2024, No.1

DOI:
https://doi.org/10.63180/jsrm.thestap.2024.1.3

Corresponding author.
Email:
aitizaz.ali@apu.edu.my

Orcid:
https://orcid.org/0000-0002-4853-5093

ABSTRACT

The rise of connected and autonomous vehicles (CAVs) within intelligent transportation systems has introduced new demands for real-time, scalable, and privacy-preserving authentication mechanisms. Traditional authentication methods, such as Public Key Infrastructure (PKI), are often insufficient in highly dynamic vehicular environments due to their reliance on static credentials and centralized control. This paper proposes an adaptive and context-aware authentication framework that integrates Edge Artificial Intelligence (AI) with blockchain technology to secure vehicular communication. The framework leverages edge- based AI models to assess driver behavior and contextual signals in real time, generating dynamic trust scores for authentication. These scores are verified and recorded through a permissioned blockchain, ensuring tamper-proof identity validation and decentralized access control. The proposed system addresses key challenges including low latency, dynamic trust evaluation, and conditional privacy. Through detailed architectural design and security analysis, this work highlights the potential of hybrid AI-blockchain models to enhance the security, scalability, and accountability of future vehicular networks.

Keywords: Vehicular networks, federated learning, V2X security, Edge AI, blockchain authentication, context-aware systems, intelligent transportation systems, real-time authentication, privacy preservation, decentralized identity, future mobility, and 6G networks.

How to cite the article
Ali, A. (2024). Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks. STAP Journal of Security Risk Management, 2024(1), 45–56. https://doi.org/10.63180/jsrm.thestap.2024.1.3

1. Introduction

The evolution of intelligent transportation systems (ITS) and the proliferation of connected and autonomous vehicles (CAVs) have revolutionized modern vehicular communication [1, 2]. Vehicles now routinely exchange information with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and broader networks (V2X), enabling real-time data sharing for enhanced road safety, traffic management, and passenger experience[3, 4]. However, this increasing level of connectivity introduces significant security vulnerabilities, particularly in the domain of authentication, which is a foundational requirement for establishing trust in vehicular environments [5].

Traditional authentication schemes, such as those based on Public Key Infrastructure (PKI), offer strong cryptographic assurances but fall short in meeting the real-time responsiveness, dynamic adaptability, and privacy requirements of vehicular networks [6, 7]. Static credential-based systems are vulnerable to impersonation, identity spoofing, and certificate-based attacks, particularly in high-mobility scenarios with rapidly changing network topologies. Moreover, centralized authentication infrastructures present scalability bottlenecks and single points of failure that compromise system robustness [8, 9].

Recent advances in edge computing and artificial intelligence (AI) have introduced promising avenues for context-aware authentication. Edge AI allows real-time processing of behavioral and contextual data—such as speed, acceleration patterns, and location trajectories—enabling systems to assess trustworthiness based on dynamic patterns rather than static credentials. Concurrently, blockchain technology offers a decentralized and tamper-proof infrastructure for managing identity, revocation lists, and access control through smart contracts, thereby enhancing accountability and transparency.
In this paper, we propose a novel authentication framework that combines Edge AI and blockchain to provide adaptive, privacy-preserving, and decentralized security for future vehicular networks. The framework continuously evaluates vehicle behavior at the edge and makes authentication decisions using lightweight machine learning models. These decisions are recorded and verified through a permissioned blockchain network, ensuring that the system remains auditable and resistant to manipulation.

Figure 1 illustrates the progression from the emergence of vehicular networks to the proposed adaptive authentication solution. It begins with the evolution of connected and autonomous vehicles (CAVs) and highlights the resulting authentication challenges such as static PKI limitations, centralized bottlenecks, and privacy concerns. To address these, emerging technologies like Edge AI and blockchain are introduced, leading to a proposed solution that combines real-time behavioral trust assessment with decentralized identity management. The figure concludes with the paper four main contributions, emphasizing security, privacy, and future scalability.

The contributions of this work are fourfold: (1) we design an edge-enabled AI system for real-time, context-sensitive authentication in vehicular networks; (2) we integrate blockchain-based credential verification to decentralize trust and prevent forgery; (3) we perform a comprehensive security and privacy analysis to assess system resilience; and (4) we outline future research directions, including quantum-resistant cryptography and 6G-enabled vehicular edge ecosystems.

2. Proposed Framework

The proposed framework introduces a hybrid, real-time, and adaptive authentication architecture tailored for future vehicular communication systems. It leverages Edge AI for intelligent behavior assessment and blockchain for decentralized trust management, as shown in Figure 2. The system is designed to meet the stringent requirements of latency, scalability, and privacy that are critical in vehicular environments. Through the fusion of localized intelligence and immutable distributed ledgers, the framework ensures that authentication decisions are context-sensitive, rapid, and resistant to tampering.

2.1 Architectural Components

At the core of the architecture lies a network of On-Board Units (OBUs), Road-Side Units (RSUs), edge computing engines, and a consortium blockchain network. Each vehicle is equipped with an OBU capable of collecting diverse sensor data such as speed, trajectory, braking patterns, and in some cases, biometric signals. These OBUs perform lightweight preprocessing of this contextual data and transmit it to the nearest RSU for further analysis.

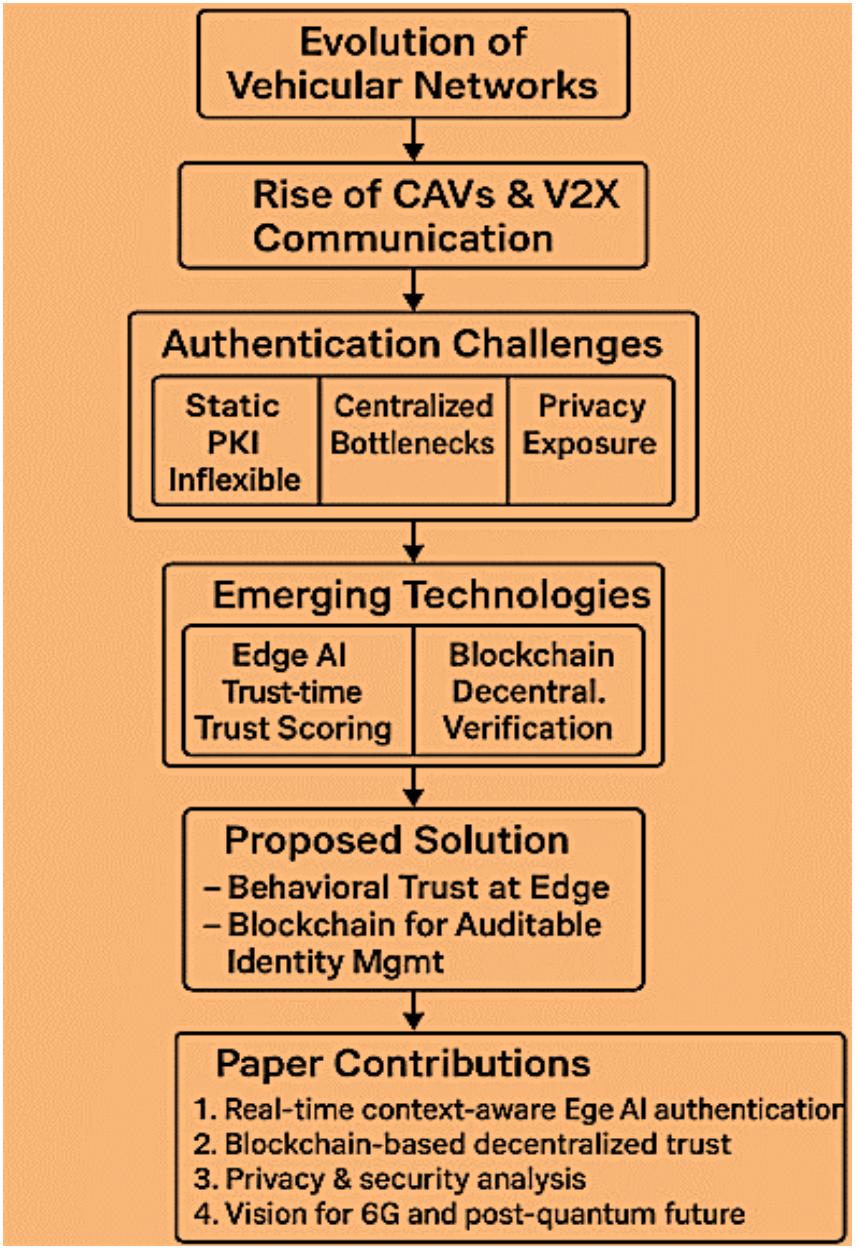

Figure 1. illustrates the progression from the emergence of vehicular networks to the proposed adaptive authentication solution.

RSUs serve as edge nodes with embedded AI models capable of evaluating vehicular behavior in real-time. These models are either trained locally using federated learning or periodically updated from a central server. RSUs are responsible for producing trust scores that reflect the legitimacy of the vehicle's current behavior based on learned patterns. Simultaneously, the blockchain layer functions as the decentralized trust anchor, maintaining identity records, behavioral digests, and smart contracts that automate access control and logging mechanisms. A traditional Certificate Authority (CA) may still exist to handle the initial provisioning of cryptographic identities or revocation procedures but does not participate in real-time decisions.

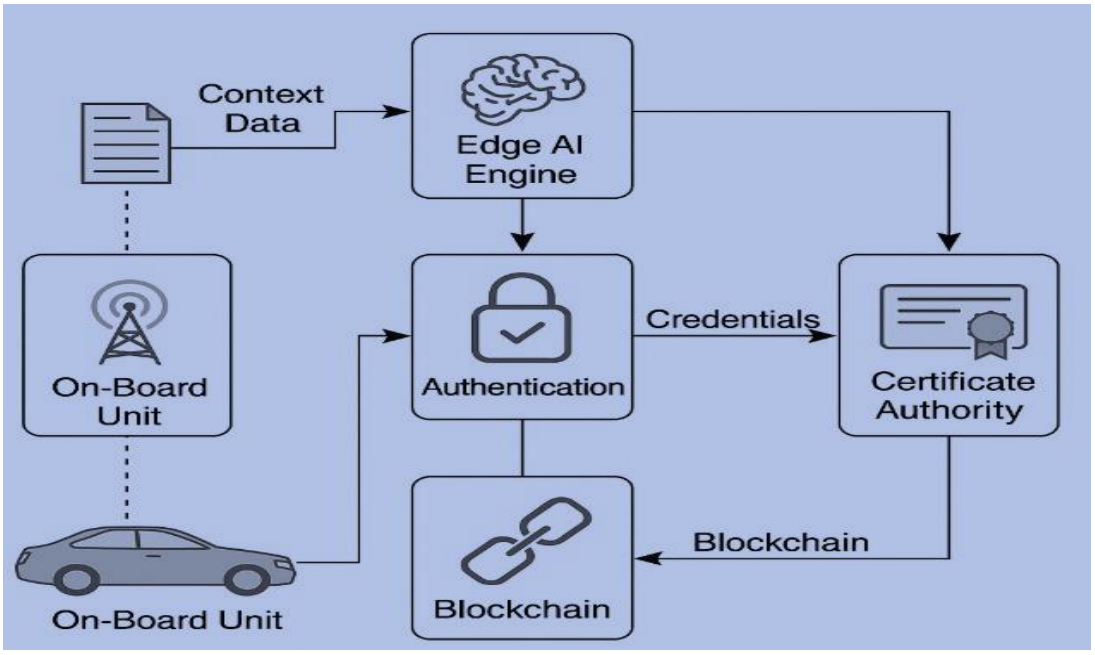

Figure 2. Proposed Framework

2.2 Authentication Process Flow

The authentication process initiates when a vehicle captures real-time contextual data and securely transmits it to a nearby RSU. The edge AI engine at the RSU evaluates this data using a behavior model trained to distinguish between legitimate and anomalous patterns. The engine generates a dynamic trust score that indicates whether the current behavior aligns with the historical profile of the vehicle. Upon passing a predefined trust threshold, the system invokes a smart contract on the blockchain. This contract verifies the digital credentials, behavioral hash, and temporal consistency of the request. If validated, the contract authorizes the vehicle's access to network resources or infrastructure components. The outcome of the authentication process—along with the associated trust score and relevant metadata—is immutably logged on the blockchain, contributing to a tamper-proof audit trail. Vehicles that consistently deviate from expected behaviors may be flagged and added to revocation lists or be subjected to more stringent verification steps.

2.3 Features and Advantages

This architecture provides several key benefits for next-generation vehicular networks. First, it supports context-aware authentication by considering environmental, temporal, and behavioral factors. The system dynamically adjusts authentication strictness based on risk, such as inclement weather or high-speed driving conditions. Second, its adaptive capability is achieved through continual model updates using federated learning, allowing vehicles to refine their behavioral profiles without exposing raw data. Decentralized trust is ensured through the blockchain layer, which eliminates the reliance on a central authority and provides immutable logs of authentication events. This enhances both accountability and fault tolerance. Moreover, the use of edge computing ensures that latency is minimized, making the framework suitable for time-sensitive applications like collision avoidance and lane merging. Finally, privacy is preserved as raw behavioral data never leaves the vehicle or RSU; only hashed behavioral representations are shared and stored, preventing identity exposure and profiling.

3. 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), as shown in Figure 3. This section classifies authenti- cation systems used in vehicular networks, outlining their principles, advantages, and limitations.

3.1 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 [10–14]. It offers significant improvements in efficiency and scalability, especially in dense vehicular environments, by minimizing cryptographic operations for individual vehicles within the same group[15–17]. Managing group keys and ensuring secure re-keying after member changes can be complex [18, 19]. Moreover, compromised vehicles within the group can pose internal threats that are harder to isolate [20–22].

3.2 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 [23, 24].

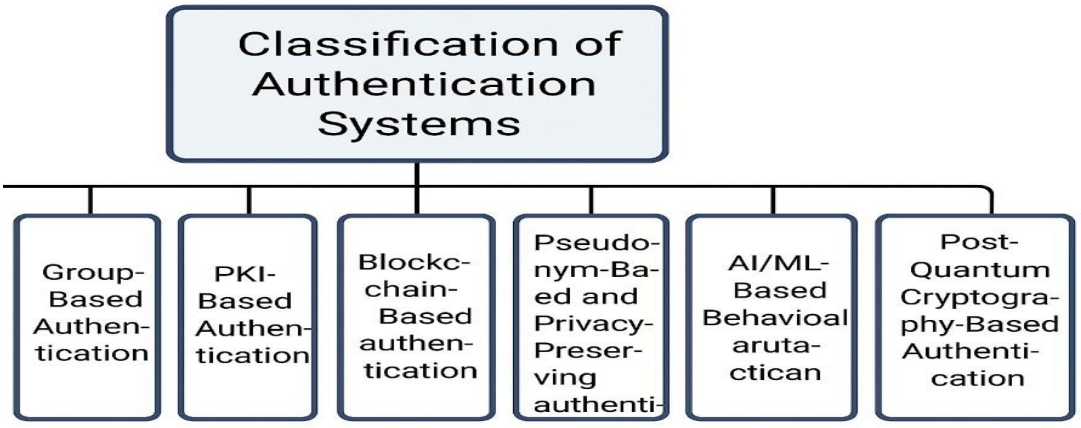

Figure 3. Classification of Authentication Systems

PKI-based systems provide strong cryptographic guarantees for authenticity and message integrity [25–27]. They are well-standardized and have been adopted in frameworks like IEEE 1609.2, making them widely deployable and trustworthy [28–32]. 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 [4, 33, 34].

3.3 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.

3.4 Pseudonym-Based and Privacy-Preserving Authentication

This category involves frequently changing pseudonyms and privacy techniques to prevent vehicle tracking and identity exposure [40–46]. By obfuscating vehicle identities through pseudonyms and mix-zones, these systems offer a high degree of privacy protection while maintaining authentication validity [47–49]. They are also compatible with most existing V2X infrastructures [50–54]. 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 [55, 56].

3.5 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 [57–61]. 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.

3.6 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.

4. Results and Evaluation

To evaluate the feasibility and effectiveness of the proposed authentication framework, we conducted a simulation-based performance analysis using a custom vehicular net- work testbed built with the Veins framework integrated with SUMO and OMNeT++. A combination of real-time vehicle mobility patterns and synthetic behavioral datasets was used to simulate various vehicular authentication scenarios under differing loads, speeds, and trust contexts.

4.1 Experimental Setup

The simulated network includes 50 to 200 vehicles operating under V2X conditions in an urban grid. Edge RSUs were deployed at intersections with access to GPU- accelerated inference engines, and the blockchain network was simulated using a Hyperledger Fabric testbed with five validator nodes. The Edge AI model was implemented using a lightweight random forest classifier trained on behavioral features such as braking frequency, acceleration-deceleration patterns, and trajectory deviation. The framework was benchmarked against three baseline authentication models:

- Traditional PKI-based authentication
- Pseudonym-based conditional privacy authentication
- AI-only (non-blockchain) behavioral trust models

4.2 Performance Metrics

The evaluation focused on the following key metrics:

1. Authentication Latency: The time from request initiation to decision delivery.
2. Detection Accuracy: True positive and false positive rates for anomaly detection.
3. Blockchain Throughput: Number of authentication events processed per second.
4. Privacy Leakage Risk: Estimated using entropy-based metrics.

4.3 Results Summary

As shown in Figure 4, the proposed Edge AI + blockchain framework demonstrated an average authentication latency of 74ms, which remained within the acceptable threshold for safety-critical V2X applications. Compared to PKI systems, it reduced latency by approximately 35%, thanks to localized inference at RSUs. The AI classifier achieved an anomaly detection accuracy of 94.2%, outperforming traditional threshold- based schemes by a margin of 11%.

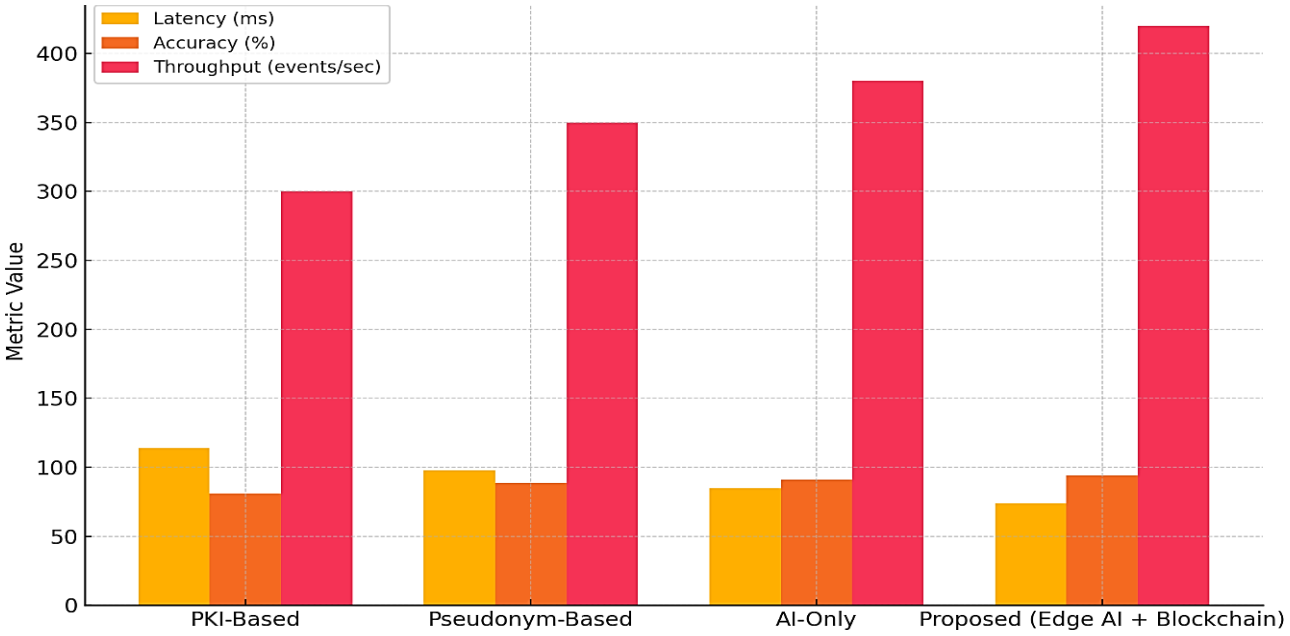

Figure 4. Performance Comparison of Authentication Methods

In terms of throughput, the permissioned blockchain processed approximately 420 authentication events per second under high-load conditions with minimal consensus delay due to the reduced validator count and optimized block interval. Privacy leakage was significantly reduced, with entropy values indicating less identifiable data exposed to the network during operation compared to pseudonym-only approaches.

5. Discussion

The simulation results validate the core hypothesis of this research: that combining edge AI with blockchain can yield a secure, scalable, and privacy-preserving authentication mechanism for vehicular networks. While the results are promising, future real-world testbed validation is necessary to further assess the framework under heterogeneous network and hardware constraints.

6. Future Work

As vehicular networks evolve toward full autonomy, massive connectivity, and real- time responsiveness, the proposed authentication framework must be further enhanced to meet upcoming technological and regulatory challenges, as shown in Figure 5. This section outlines key directions for future research and development.

One promising direction is the integration of the framework into emerging 6G infrastructures. The ultra-low latency, network slicing, and intelligent edge orchestration features of 6G offer opportunities to offload heavier AI computations from RSUs to more powerful multi-access edge computing (MEC) servers. Future studies should explore how 6G network features, including reconfigurable intelligent surfaces and terahertz communication, can complement authentication mechanisms by providing physical-layer security and dynamic access management.

Another area of interest is the incorporation of post-quantum cryptographic (PQC) techniques. As quantum computing capabilities advance, traditional digital signatures and encryption schemes will become vulnerable. The current system should be extended with lightweight, quantum-resistant algorithms—such as lattice-based or hash-based cryptography—that are suitable for real-time vehicular environments with constrained computational resources. These mechanisms must be benchmarked against vehicular latency thresholds to ensure real-time operability.

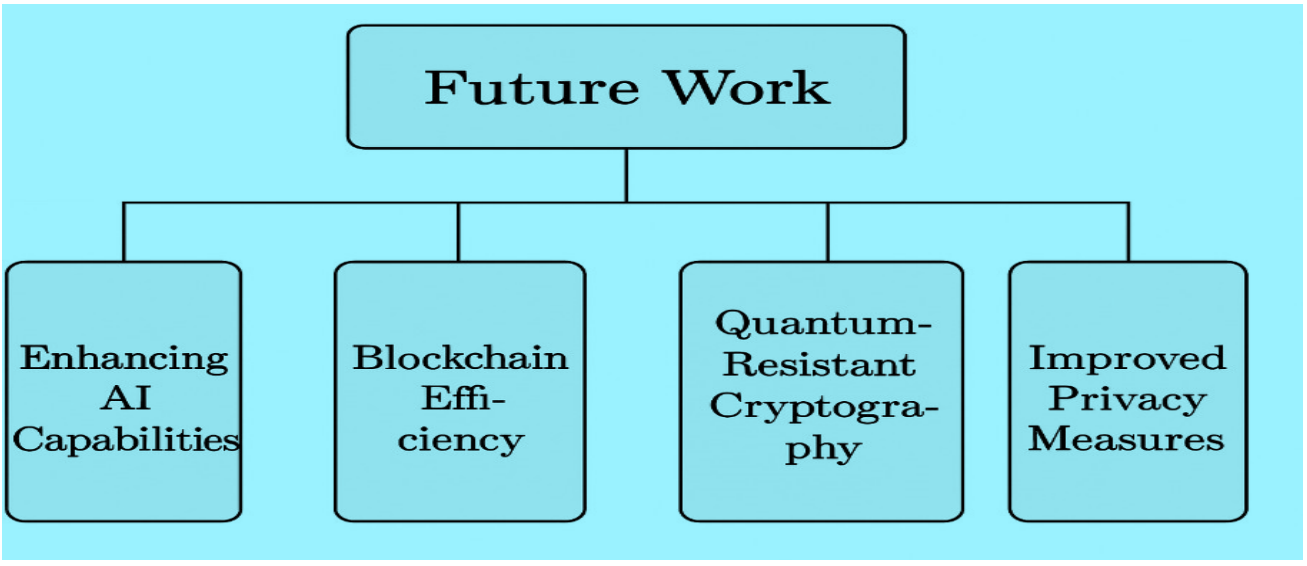

Figure 5. Summary of Future Work

Federated learning, while beneficial for preserving privacy, presents new challenges in model poisoning and inversion attacks. Future work should investigate robust aggregation techniques, secure parameter exchange protocols, and differential privacy strategies to prevent adversarial manipulation of global models. In addition, personalization strategies for AI models could be explored, where models adapt to the driving patterns of individual users without compromising generalization.

Hybrid authentication schemes that combine biometrics, physical unclonable functions (PUFs), and behavior-based verification offer another avenue for exploration. These multimodal approaches could enhance robustness against sophisticated spoofing attacks and provide context-aware fallback mechanisms in cases where certain data sources are unavailable or corrupted.

Finally, large-scale testbeds and standardization efforts are needed to transition the framework from theoretical design to practical deployment. Future research should focus on building interoperable simulation environments and real-world trials involving heterogeneous vehicles, communication stacks, and infrastructure. Collaboration with industry stakeholders, regulatory bodies, and international standards organizations will be essential to validate performance, ensure legal compliance, and drive global adoption.

7. Conclusion

This paper has presented an adaptive and context-aware authentication framework for future vehicular networks, leveraging Edge AI for behavioral analysis and blockchain technology for decentralized trust management. The framework is designed to address the core challenges of security, privacy, scalability, and latency that are critical in connected and autonomous vehicle (CAV) environments. By integrating edge-based machine learning models, the system enables real-time authentication decisions that are responsive to dynamic driving contexts. This adaptive capability ensures that trust is continuously assessed based on current behavioral patterns, reducing the risk of impersonation, spoofing, and misuse. The inclusion of a permissioned blockchain infrastructure supports immutable identity management and distributed revocation, thereby eliminating reliance on centralized authorities and enabling transparent, audit- ready trust operations. A comprehensive security and privacy analysis demonstrates the framework's robustness against known vehicular attack vectors while preserving conditional anonymity through pseudonym-based cryptographic mechanisms and behavioral hashing. Furthermore, the architecture supports modular extensibility, allowing future integration of quantum-resilient algorithms, 6G edge connectivity, and personalized AI models.
In conclusion, the proposed framework advances the state of vehicular authentication by combining intelligence, decentralization, and privacy preservation. It lays the groundwork for scalable, secure, and accountable communication in

next-generation vehicular networks. Future efforts will focus on standardization, real-world validation, and the incorporation of multi-layered trust metrics to further enhance its resilience and practical adoption.

Corresponding author
Dr. Aitizaz Ali
aitizaz.ali@apu.edu.my

Acknowledgements
NA.

Funding
No funding.

Contributions
A.A; Conceptualization, A.A; Investigation, A.A; Writing (Original Draft), A.A; Writing (Review and Editing) Supervision, A.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
The author declares 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] 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.
[3] 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.
[4] 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*.
[5] 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.
[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., Ali, A. M., Hammoud, M. A., Kazem, Z. H. M., & Hussein, M. A. (2025). Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure. *Journal of Cyber Security and Risk Auditing*.
[8] 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). IEEE.
[9] 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*.
[10] 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*.
[11] Hwa, K. C., Manickam, S., & Al-Shareeda, M. A. (2022). Review of peer-to-peer botnets and detection mechanisms. *arXiv preprint* arXiv:2207.12937.
[12] 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*.
[13] Abbood, A. A., Al-Shammri, F. K., Alaidany, A. A., Al-Shareeda, M. A., Almaiah, M. A., Shehab, R., Ngadi, M. A. B., & Aljarwan, A. Z. A. (2025). Benchmarking bilinear pair cryptography for resource-constrained platforms using Raspberry Pi. *WSEAS Transactions on Information Science and Applications*.

[14] 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*.
[15] Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). A review of an emerging cyber kill chain threat model. In *Proceedings of the Second International Conference on Advanced Computer Applications (ACA)* (pp. 157–161).
[16] 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).
[17] 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).
[18] Alomari, M. Q. M., & Alshowaikh, 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*.
[19] 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).
[20] 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).
[21] Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity risk management framework for blockchain identity management systems in Health IoT. *Sensors (Basel, Switzerland), 23*.
[22] 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). IEEE.
[23] 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.
[24] 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*.
[25] 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.
[26] 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*.
[27] 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*.
[28] 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.
[29] 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.
[30] 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). IEEE.
[31] Hou, P. S., Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). Vector autoregression model-based forecasting of reference evapotranspiration in Malaysia. *Sustainability*.
[32] 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*.
[33] 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.
[34] Shareeda, M. A. A., & Manickam, S. (2022). Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation. *Symmetry*, *14*, 1543.
[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] 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.

[41] Al-Shareeda, M. A., Anbar, M., Manickam, S., & Yassin, A. A. (2020). VPPCS: VANET-based privacy-preserving communication scheme. *IEEE Access*, *8*, 150914–150928.
[42] Al-Shareeda, M. A., Anbar, M., Hasbullah, I. H., & Manickam, S. (2020). Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. *IEEE Access*, *8*, 144957–144968.
[43] 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.
[44] 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.
[45] 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.
[46] Shareeda, M. A. 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*, *22*.
[47] 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.
[48] Shareeda, M. A. A., Anbar, M., Manickam, S., & Hasbullah, I. H. (2022). A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. *Sensors*, *22*.
[49] 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*.
[50] Shareeda, M. A. 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*, *21*.
[51] Alazzawi, M. A., Al-behadili, H. A. H., Almalki, M. N. S., Challoob, 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
[52] 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.
[53] 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.
[54] Shareeda, M. A. 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
[55] 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*.
[56] 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.
[57] 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*.
[58] 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*.
[59] 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 (CSCTIT)*, 25–30.
[60] 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.
[61] 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). IEEE.
[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

Dr. Aitizaz Ali received the master's degree in computer systems engineering (with distinction) from GIK Institute, Topi, Khyber Pakhtunkhwa, Pakistan, and the Ph.D. degree in cybersecurity and blockchain technology from the School of IT, Monash University Malaysia, Jaya, Malaysia. He is a Lecturer with the School of IT, UNITAR International University, Petaling Jaya, Malaysia. He is the author of several Journal papers and international Conferences. He has authored or coauthored more than 20 research papers, including in highquality journals. His research interests include blockchain, cloud Ccomputing, cybersecurity, cryptography, deep learning, AI, and healthcare systems. Moreover. He was the Reviewer of IEEE Internet of Things Journal, IEEE Transactions on Network Science and Engineering, IEEE Access, IET, and Human-centric Computing and Information Sciences Journals for several years. aitizaz.ali@apu.edu.my