Available on: http://gjetr.ep-journals.org/ E-ISSN: 3051-3782, P-ISSN: 3051-3774

Global Journal of Engineering and Technology Review
Volume: 02 Issue: 08 August 2026

A Hybrid Post-Quantum Cryptography and Machine Learning Framework for Intrusion Detection in VANETs

Moses O. Bankole
Bath Spa University, University of East London, University of the west Scotland

Published Date: August 03, 2026 **Article DOI : 10.65150/EP-gjetr/V2E8/2026-03**

ABSTRACT: Vehicular Ad Hoc Networks (VANETs) are a fundamental technology for intelligent transportation systems, enabling real-time communication between vehicles, roadside infrastructure, and cloud-based services. However, the increasing connectivity of vehicles introduces significant cybersecurity challenges, including replay attacks, Sybil attacks, false message injection, and denial-of-service attacks. Existing VANET security mechanisms primarily rely on conventional cryptographic algorithms such as RSA and ECC, which are vulnerable to future quantum computing threats. Furthermore, traditional intrusion detection systems lack the intelligence and adaptability required to detect evolving cyber threats in highly dynamic vehicular environments.

This paper proposes a Hybrid Post-Quantum Cryptography and Machine Learning Framework for Intrusion Detection in VANETs (HPQC-ML-VANET). The proposed framework integrates post-quantum cryptographic mechanisms based on lattice-based algorithms with a machine learning-driven intrusion detection system. The cryptographic layer provides quantum-resistant authentication and secure key exchange, while the machine learning layer performs behavioural analysis and real-time anomaly detection. The proposed approach combines CRYSTALS-Kyber for secure key encapsulation and CRYSTALS-Di lithium for digital authentication with a hybrid machine learning model based on feature extraction, dimensionality reduction, and ensemble classification.

The framework is evaluated using simulated VANET communication environments incorporating realistic vehicle mobility and cyberattack scenarios. Performance evaluation considers detection accuracy, false positive rate, communication overhead, and detection latency. The proposed framework aims to provide a scalable, privacy-preserving, and quantum-resistant security solution for future autonomous and connected vehicles.

KEYWORDS: Post-Quantum Cryptography, VANET, Intrusion Detection System, Machine Learning, Cybersecurity, Autonomous Vehicles, CRYSTALS-Kyber, CRYSTALS-Di lithium.

1. INTRODUCTION

The emergence of connected and autonomous vehicles has transformed modern transportation systems by enabling intelligent communication between vehicles and infrastructure. Vehicular Ad Hoc Networks (VANETs) support applications such as collision avoidance, traffic management, emergency communication, and autonomous driving.

Despite these advantages, VANETs introduce significant security vulnerabilities due to their open wireless communication environment. Unlike traditional networks, vehicles operate in highly dynamic conditions where nodes frequently join and leave communication networks. According to the research, almost one-third of the people in the developed world have a vehicle license to drive cars. The vehicles in VANET use wireless technology, such as 5G, that enables attackers to attack the network using its open nature. As a prevention to this attack, misbehaviour detection [1]. systems are developed to attack and prevent these behaviours. The prevention only captures the incoming data packets and provides an easy way to enable these attackers to catch and enlist them for distribution. Many attacks on the VANET environment can hack the network [2]

The VANET term is implemented from the autonomous network transformation to im plement the nature of the wireless network. It holds the new generation of technologies that embrace the nature of network deployment and provides the ability to enhance knowledge and experience of network boundaries. The idea of the VANET is that it connects in the same way as the computing connectivity of mobile devices. These devices are connected to deploy the proper network architecture. Intelligent Transportation System (IST) is one of the key deployment [3] areas that makes the network architecture more secure and provides reliable features and delivery services for the network's needs. In VANET, we contain three types of communications, i.e., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I) communication [4].

In the past, vehicle systems, traffic infrastructure systems, and service providers operated independently. However, with the advent of ITS, these systems must interact and exchange information. The data exchanged encompasses a broad spectrum of information, including, but not limited to, traffic information, map descriptions, and traffic light status. It also includes accident reports, routing information, emergency services, cooperative driving, and safety-relevant data intended to prevent accidents. Furthermore, data pertaining to management and security will be exchanged [5]. This creates opportunities for malicious actors to exploit communication channels.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

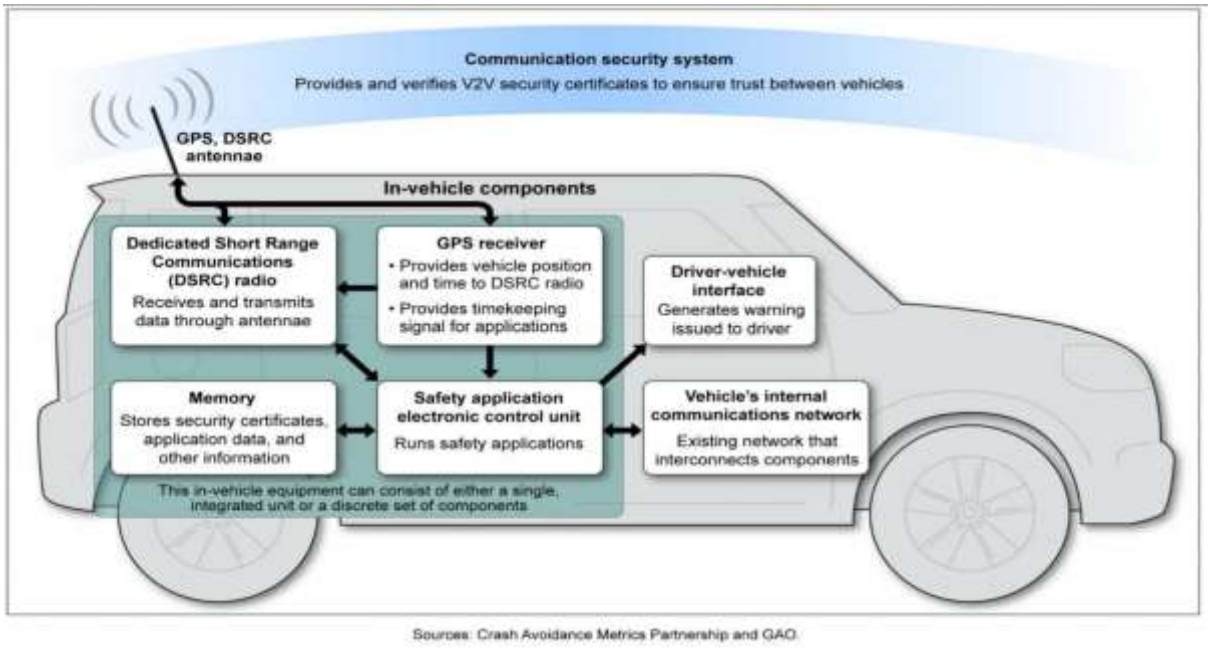
Common VANET attacks include:

- Replay attacks
- Sybil attacks
- Message modification
- Identity spoofing
- Denial-of-Service attacks

Traditional VANET security mechanisms use public-key cryptography, including RSA and Elliptic Curve Cryptography (ECC) [6]. However, advances in quantum computing threaten these cryptographic systems. Shor's algorithm enables quantum computers to efficiently solve integer factorisation and elliptic curve discrete logarithm problems, making current security mechanisms ineffective against future quantum attacks [7]. Therefore, there is a critical requirement for quantum-resistant security solutions.

Post-Quantum Cryptography (PQC) provides cryptographic algorithms designed to withstand attacks from quantum computers. However, implementing PQC alone does not solve the challenge of intelligent cyberattack detection. Machine Learning (ML) techniques provide powerful capabilities for identifying abnormal communication patterns and detecting unknown attacks [8] [9]

This research proposes a hybrid framework combining PQC and ML-based intrusion detection to improve VANET security.



2. RELATED WORK

2.1 DSRC and Wireless Access in Vehicular Environments: DSRC is a set of standards that facilitate the transmission of messages with relatively secure and high-speed communications, low latency, and fast network connectivity in V2X communications. The IEEE 802.11p standard, on which WAVE communications are based, guarantees that high-priority communications will not experience delays of more than tens of milliseconds [10]. An attacker may acquire accessibility to the broadcast timetable, which is employed to transmit service notifications and broadcast messages at the same time, resulting in a communication conflict that will go unnoticed by vehicle drivers. In [11], the authors describe the challenges to WAVE service advertisement (WSA). They conclude that WSA is susceptible to attacks on both its accessibility and its security.

2.2 VANET Security Challenges

VANET communication relies on wireless channels that expose vehicles to various attacks. Existing security solutions focus mainly on authentication and encryption but often fail to provide intelligent threat detection.

The deployment of a security system for VANET is challenging. In fact, the highly dynamic nature with frequent disconnection, instantaneous arrivals and departures of vehicles, the usage of wireless channels to exchange emergency and safety messages, expose VANETs to various threats and attacks. In this section, we will classify the attacks, the attackers and analyse which VANET communication mode they affect [12].

2.3 Machine Learning-Based VANET Intrusion Detection

Machine learning has been widely applied for network intrusion detection.

Common approaches include:

Algorithm	Advantage
Random Forest	High classification accuracy
SVM	Effective binary classification
XGBoost	Strong performance with complex data
Neural Networks	Detect nonlinear patterns
Autoencoders	Feature reduction and anomaly detection

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

However, existing ML-based IDS approaches suffer from:

- High false-positive rates
- Lack of privacy protection
- Dependency on centralised training
- Vulnerability to future quantum attacks

2.4 Post-Quantum Cryptography in VANET

Recent research has investigated PQC algorithms for future vehicle communication.

PQC-based frameworks primarily focus on cryptographic primitives such as key exchange and digital signatures without incorporating trust enforcement or audit mechanisms. Blockchain-integrated Zero Trust architectures provide decentralized auditability and access control but typically remain cryptography-agnostic and do not incorporate post-quantum protection. Machine learning–based Zero Trust enforcement improves adaptive policy generation but does not address cryptographic resilience against quantum adversaries. Similarly, homomorphic encryption–based approaches support privacy-preserving computation but introduce significant latency overheads that limit their applicability in real-time healthcare environments [13].

The NIST PQC standardisation process identified lattice-based algorithms as promising candidates.

This research adopts:

CRYSTALS-Kyber

For:

- Secure session establishment
- Key exchange

CRYSTALS-Di lithium

For:

- Vehicle authentication
- Digital signatures

3. PROPOSED FRAMEWORK

The proposed HPQC-ML-VANET framework consists of four layers:

3.1 Vehicle Communication Layer

Each vehicle contains:

- On-board unit (OBU)
- Sensors
- Communication module
- Security agent

Vehicles exchange safety messages:

$$M_i = (I, D_i, L_i, T_i D_i)$$

where:

ID = vehicle identity
L = location
T = timestamp
D = message data

3.2 Post-Quantum Security Layer

The framework performs secure authentication before communication.

Key Exchange

Kyber generates a shared secret:

$$(p, ksk) = KeyGen(\ \ )$$

Encapsulation:

$$(C, K) = Encaps(pk)$$

Decapsulation:

$$K = Decaps(s, kC)$$

The shared key protects vehicle communication.

Authentication

Di lithium generates signatures:

$$\sigma = Sign(s, kM)$$

Verification:

$$Verify(p, k, M\sigma)$$

Only authenticated vehicles can participate.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

3.3 Machine Learning Intrusion Detection Layer

The IDS pipeline consists of:

3.4 Attack Detection Model

The system detects:

Replay Attack

Detected using timestamp behaviour:

$$T_c - T_r > Threshold$$

where:

Tc = current timestamp

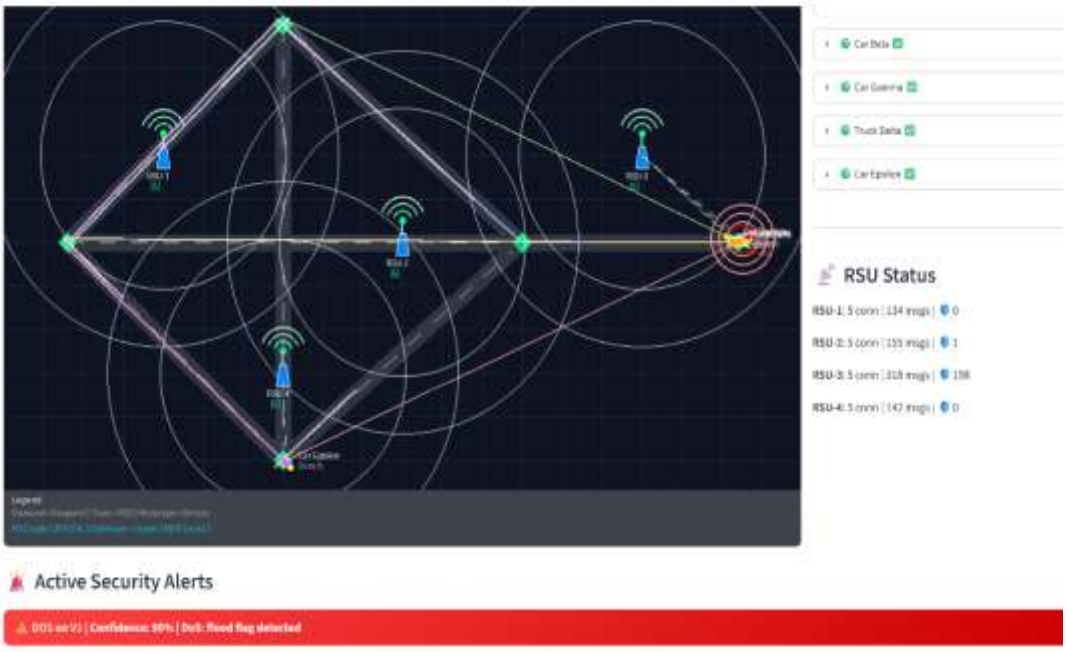
Tr = received timestamp

4. RESEARCH METHODOLOGY

The research follows a design science methodology:

Phase 1: Security Requirement Analysis

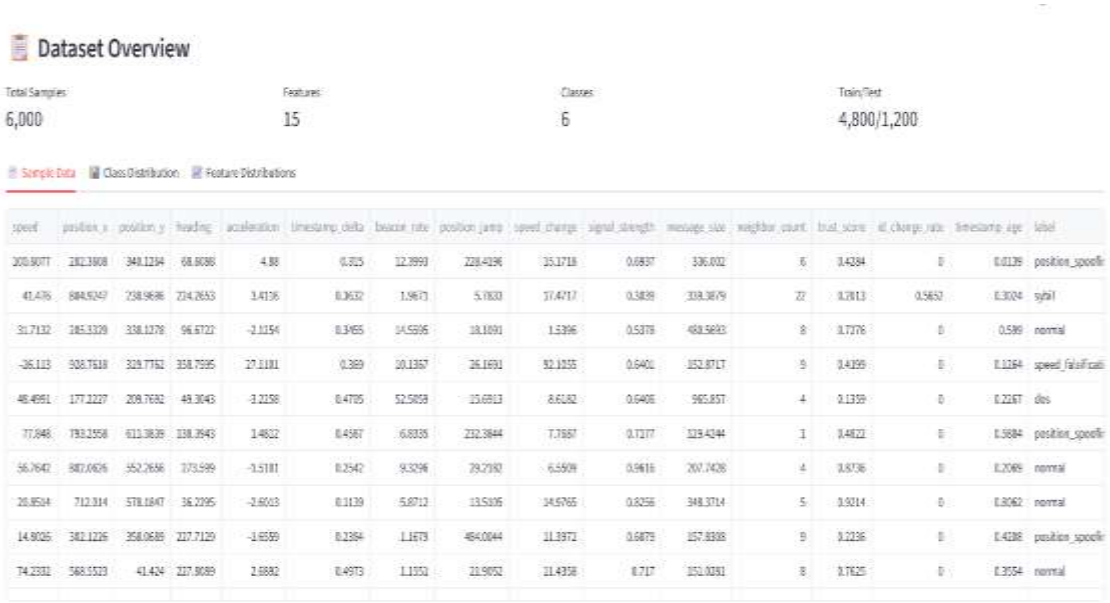
Identify VANET vulnerabilities.



Phase 2: Framework Development

Develop:

- PQC security module
- ML intrusion detection model



License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Phase 3: Simulation

Environment:

Python stream lit



Phase 4: Evaluation

Metrics:

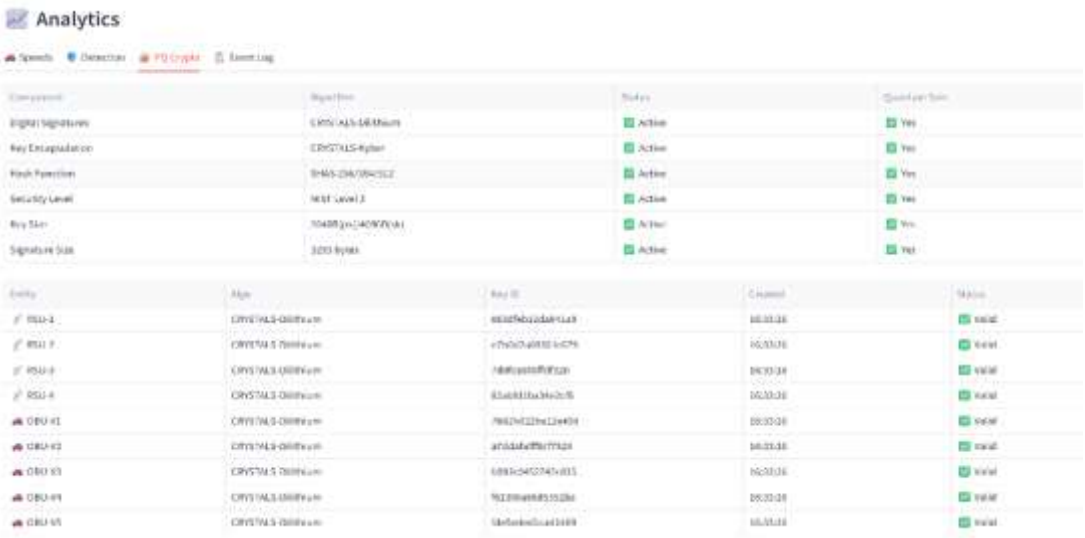
- Accuracy
- Precision
- Recall
- F1-score
- Latency
- Communication overhead



5. EXPERIMENTAL SETUP



License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/



Simulation Environment

Component	Tool
Network Simulation	NS-3
VANET Framework	Veins
ML Development	Python
PQC Library	Open Quantum Safe

6. EXPECTED RESULTS AND DISCUSSION

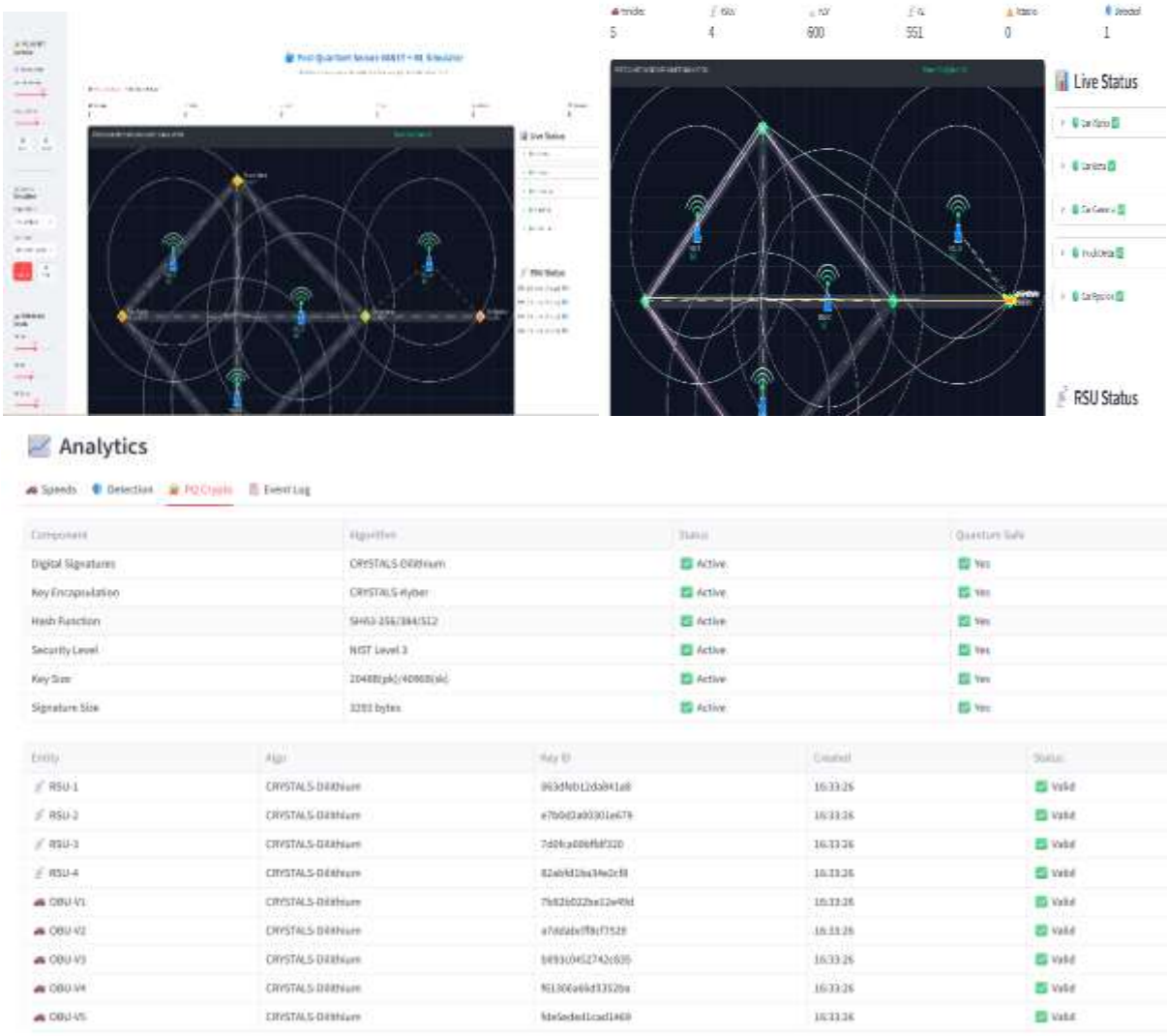
The proposed framework is expected to achieve:

Metric	Expected Improvement
Detection accuracy	>95%
False alarm reduction	Improved
Authentication security	Quantum resistant
Communication overhead	Optimised
Detection latency	Suitable for real-time VANET



License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

The hybrid approach provides advantages over traditional IDS approaches because it combines proactive cryptographic protection with intelligent attack detection.



7. RESEARCH CONTRIBUTIONS

This research contributes:

Contribution 1

A hybrid PQC and ML security architecture for VANET environments.

Contribution 2

Integration of quantum-resistant authentication using Kyber and Di lithium.

Contribution 3

Machine learning-based detection of dynamic VANET attacks.

Contribution 4

A scalable security framework suitable for future autonomous vehicles.

8. CONCLUSION

This paper presented a Hybrid Post-Quantum Cryptography and Machine Learning Framework for Intrusion Detection in VANETs. The proposed solution addresses two major challenges facing future connected vehicles: quantum computing threats and intelligent cyberattacks.

By combining lattice-based post-quantum cryptography with machine learning-based intrusion detection, the proposed framework provides secure authentication, anomaly detection, and adaptive cyber defence. Future work will focus on implementing the framework using python stream lit simulation and evaluating performance against advanced VANET attacks.

REFERENCES

1) Al-Omaisi, H.; Sundararajan, E.A.; Abdullah, N.F. Towards vanet-ndn: A framework for an efficient data dissemination design scheme. In Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI), Bandung, Indonesia, 9–10 July 2019; pp. 412–417.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

2) Pournaghi, S.M.; Zahednejad, B.; Bayat, M.; Farjami, Y. NECPPA: A novel and efficient conditional privacy-preserving authentica tion scheme for VANET. Comput. Networds 2018, 134, 78–92.
3) Vogt, J., Schotten, H.D. and Wieker, H., 2025. Intelligent transportation system protocol interoperability evaluation. IEEE Open Journal of Intelligent Transportation Systems, 6, pp.67-94.
4) Lee, M.; Atkison, T. Vanet applications: Past, present, and future. Veh. Commun. 2021, 28, 100310.
5) European Commission https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en .
6) Mohammed, Z.K., Mohammed, M.A., Ghani, M.K.A., Aliesawi, S.A., Lakhan, A., Abdulkareem, K.H., Marhoon, H.A. and Al-Andoli, M.N., 2025. Privacy-preserving communication in smart city transportation using elliptic curve cryptography. Scientific Reports, 15(1), p.34342.
7) Dorojan, V., 2025. A General Introduction to Shor's Algorithm and Its Applications. Available at SSRN 5181944.
8) Sharma, A. and Rani, S., 2025. Post-quantum cryptography (PQC) for IoT-consumer electronics devices integrated with deep learning. IEEE Transactions on Consumer Electronics.
9) John, B., 2025. Machine Learning-Based Anomaly Detection in V2V and V2X Networks.
10) K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, “Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–performance evaluation,” Transp. Res. C, Emerg. Technol., vol. 68, pp. 168–184, Jul. 2016.
11) W. Whyte, J. Petit, V. Kumar, J. Moring, and R. Roy, “Threat and countermeasures analysis for WAVE service advertisement,” in Proc. IEEE 18th Int. Conf. Intell. Transp. Syst., Sep. 2015, pp. 1061–1068.
12) Mejri, M.N., Ben-Othman, J. and Hamdi, M., 2014. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2), pp.53-66.
13) Devaraj, Poojitha, Syed Abrar Chaman Basha, Nithesh Nair Panarkuzhiyil Santhosh, and Niharika Panda. 2026. "A Post-Quantum Secure Architecture for 6G-Enabled Smart Hospitals: A Multi-Layered Cryptographic Framework" Future Internet 18, no. 3: 165. https://doi.org/10.3390/fi18030165
14) Lutz, M., 2001. Programming python. " O'Reilly Media, Inc.".
15) Khorasani, M., Abdou, M. and Fernández, J.H., 2022. Web application development with streamlit. Software Development, 498, p.507.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Corresponding Author: Moses O. Bankole