SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I6P104

Volume 12 Issue 6, 35-50, June 2025

Original Article

Quantum-Secure Predictive Maintenance Framework for Future VANET-Based Smart Transportation Systems

K. Sudharson[1]*, D. Rajalakshmi[2], S. Sridevi[3], K.C. Aarthi[3]

[1]*Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India.*
[2]*Department of Computer Science and Engineering, R.M.D. Engineering College, Tamil Nadu, India.*
[3]*Department of Computer Science and Engineering, Velammal Engineering College, Tamil Nadu, India.*

[*]*Corresponding Author : susankumar@gmail.com*

Received: 03 April 2025 Revised: 05 May 2025 Accepted: 04 June 2025 Published: 30 June 2025

Abstract - *The increasing use of Vehicular Ad-hoc Networks (VANETs) in smart transportation points to the need for solutions that are quantum-computing resistant. The usual reactive security systems in the cloud cannot handle real-time vehicle applications and fail even more when attacked by quantum technology. In this paper, the suggested framework, Quantum-Secure Predictive Maintenance (QSPM), combines quantum-safe communication with QKD, early fault detection using LSTM networks at the edge and verifiable maintenance results validated with blockchain technology. A secure connection is guaranteed with BB84, and AI at the edge helps predict when maintenance is required by analyzing instant sensor information in the QSPM framework. Maintenance schedule reminders are done automatically by smart contracts, and the system uses post-quantum cryptography for lasting security. Tests done in NS-3 and MATLAB demonstrated that QSPM finds 94.6% of faults, cuts packet loss by 42%, extends network lifetime by 38% and raises resistance to cyberattacks by 55%. Results indicate that QSPM provides better security, reduces how long a vehicle stands idle and makes it possible to use quantum-resistant maintenance for future connected vehicles.*

Keywords - *Quantum-Secure Communication, Predictive Maintenance, Vehicular Ad-hoc Networks (VANETs), Edge AI and IoT, Blockchain for Secure Data Management.*

1. Introduction

Vehicular Ad-hoc Networks (VANETs) are necessary for smart transportation systems to support communications among vehicles with each other and with infrastructure (V2I). It helps decrease road congestion, reduces accidents, and supports the function of autonomous vehicles. Yet, even with so many advantages, VANETs must address major challenges associated with their distributed and dynamic form. Challenges to transportation systems can include cyber-attacks, network failure, and vehicle issues, leading to major safety and performance problems. Since the number of connected vehicles is rising, making sure VANETs are safe and reliable is now essential [1].

A major problem in VANETs is how to protect communications. Widely used encryption methods, such as RSA and ECC, which are employed in VANETs, are now at risk from quantum computing. Because quantum computers are about to break the current cryptography methods, it is now critical to use quantum-safe ways to protect information sent between cars. Quantum Key Distribution (QKD) is a new way to send information, providing an encryption method that cannot be broken, according to quantum mechanics. Even so, it is tough to integrate QKD into vehicles because doing so involves high computational power and needs suitable infrastructure [2]. Together with security, ensuring the dependability of vehicles in VANETs is extremely important. Using old ways of maintaining vehicles, such as fixed or reactive care, usually causes unexpected faults, more costly repairs and service interruptions, all of which harm the car and put lives in danger. It has been demonstrated that predictive maintenance models, thanks to artificial intelligence and machine learning, improve the process of detecting faults by anticipating failures prior to them occurring. Those using DL have demonstrated that they can predict future faults from huge amounts of vehicle-derived data [3]. Even so, such models usually lack strong security, making it easier for cyber-attackers to interfere and produce inaccurate results. Predictive maintenance won't work safely without strong security measures. Although quantum cryptography, AI maintenance, and Blockchain are all being improved, the current solutions do not address all the security and reliability issues in VANETs. Although there are works on using quantum cryptography for secure VANETs, these studies frequently miss discussing AI and how it can help

predict maintenance needs, along with the flaws in older protocols given quantum risks [4]. In the same way, Blockchain has been studied for secure data storage, though very few ideas include its use alongside quantum-proof communication and preventive maintenance.

This research introduces a Quantum-Secure Predictive Maintenance (QSPM) framework to address these issues. Using QSPM, this research included QKD for protected messaging, predictive analytics that watches for faults in real-time and Blockchain to manage important data that cannot be changed. By integrating these technologies, QSPM aims to enhance the safety, error identification, and dependability of VANETs. Using the framework, communication is safe from quantum cyber-attacks, faults can be foreseen, and all maintenance records cannot be altered or tampered with [5]. The new framework is tested with advanced simulations and is seen to improve on previous approaches. As a result, QSPM reduces packet loss by 42%, identifies faults more accurately (94.6%) and lengthens the network's lifetime by 38%. Moreover, QSPM's security against cyberattacks improved by 55%, supporting its ability to ensure that the future of VANET-based intelligent transportation systems is secure, efficient and reliable.

2. Related Works

Lately, there has been much emphasis on ensuring Vehicular Ad-hoc Networks (VANETs) are secure during communication and as predictive maintenance. Researchers here use Quantum Cryptography, Deep Learning and Blockchain to ensure safer vehicles and improve methods for finding faults and scheduling predictive maintenance. Each section reviews what exists in that area and then clearly states where research gaps exist and how the solution adds value [6].

2.1. Communication with Security in VANETs

ECC and RSA, which are standard in Vehicular Ad-hoc Networks (VANETs), are now exposed to threats from quantum computers. Since Shor's Algorithm, a product of quantum computing can handle large numbers, protecting data using classical algorithms is now much more difficult. Quantum Key Distribution (QKD) has come to the fore as a promising way to protect communication security. Studies by Prateek and his team [7] showed that QKD is safe and reliable compared to the main alternatives. Unfortunately, most of what they studied could not be put into practical use, as they failed to explore QKD implementation methods suitable for vehicular networks. Similarly, Sharma et al. (2023) [8] suggested a mixed post-quantum cryptographic approach to improve security in VANETs. They use quantum-resistant cryptography and usual classical techniques to enhance the reliability of vehicle communication. The model proved helpful in some tests, but its high processing and memory needs made it ineffective during real-time driving. The QKD method in QSPM tackles the troubles that typically affect quantum cryptography. Because it uses BB84, QSPM supports secure connections between vehicles and infrastructure, which keeps the system fast and scalable. The result is that continuous, protected transmissions are possible in VANETs, although there are few resources for each connected vehicle.

2.2. The Use of AI for Predicting Problems in Equipment Maintenance

Early problems with autonomous vehicles are often detected using the systems developed for predictive maintenance and environmental sensing. The model developed by Kumar et al. (2023) [9] exceeded 99% accuracy when faults in Electric Vehicles (EVs) were detected with an R-CNN architecture. While detecting faults was greatly improved by this model, communicating with the cloud in real-time slowed down performance for VANET applications. When maintenance needed to be done quickly, these delays made it clear that cloud-based communication is not always effective for predictive maintenance in nations where autonomous vehicles are normal.

By contrast, Hadrian et al. (2023) [10] proposed DeepCAN, a brand-new technique to classify road types using only vehicle dynamics data obtained from the CAN bus. In contrast to old image- and radar-based systems, DeepCAN studies multivariate time-series data, covering vehicle velocity, revolutions per minute and acceleration and gets useful information about vehicle performance and its area. The approach is designed to lower dependence on image and radar data and offer an alternative when those sensors are not usable. Also, working with vehicle dynamics avoids the privacy problems in image-based data because it does not depend on place or picture data. DeepCAN brings together two important techniques for dealing with time-series data. The first process features the use of an LSTM AE to learn temporal patterns directly from the given time series data. The embeddings are sent to a Fully Convolutional Network Autoencoder (FCN AE) to make the system better able to determine the road type. The approach uses features to train the data, as an XGBoost classifier is applied to classify by putting the collected features together.

Hadrian et al. (2023) investigated each separate model piece along with the resulting mix of the approaches. The experiment proved that DeepCAN can efficiently and correctly identify the type of road, suggesting it will be useful in practice with autonomous vehicles. An important point is that the model works with sensor data about cars rather than images or radar, which may cause fewer problems and be more secure than visual sensors. Still, DeepCAN did well in its tests, but because security features were missing, it could be attacked by cybercriminals. Because of this limit, the model's dependability could suffer, especially in crucial autonomous systems.

2.3. Making Predictive Maintenance Secure with Blockchain

Ensuring that maintenance records are secure and not easily changed by using blockchain technology has been a major objective in recent research for VANETs. The authors of Lai et al. (2025) [11] proposed a blockchain system to safely preserve maintenance logs for all connected vehicles. Yet, their technique was hampered from being applied in VANETs because processing all those real-time blockchain transactions on many vehicles took too much computer power.

Much in the same way, Mritunjay Shall Peelam et al. [12] (2024) suggested a system that helps track the state of vehicles safely and transparently using Blockchain technology on ITS. This system uses federated learning to predict when vehicles need servicing and protects each user's personal data. With Blockchain, the system guarantees a reliable and safe log of maintenance work, while fed-learning predicts the timing for vehicle servicing using current sensor data. With this system, it is less likely that changes will be made to the records falsely, so the vehicle's important data is protected. However, as before, the technique had trouble processing data in real-time in low-power VANET nodes.

Alternatively, the Quantum-Secure Predictive Maintenance (QSPM) method uses AI and Quantum Key Distribution (QKD) to secure communication in predictive maintenance. Making smart contracts work with Blockchain allows QSPM to keep maintenance records untampered and easy to scale and work efficiently. Unlike other efforts, QSPM uses QKD through the BB84 protocol to avoid big computational problems in Blockchain and make key exchanges safer. Consequently, the system is efficient, scalable and secure, preventing cheating repairs, optimizing maintenance tasks and achieving top functionality even if resources are insufficient.

2.4. Integrating AI with Security in VANETs

The swift progress of Vehicular Ad-hoc Networks (VANETs) has required new security systems that are more modern than conventional, rule-based ones. Mixing artificial intelligence methods with traditional security approaches has become important to managing vehicular network security threats. Combining various AI approaches ensures that any individual algorithm's flaws are removed, providing fast threat detection in mobile locations. Ahmed et al. (2024) [13] designed an intelligent system for detecting DoS attacks in Internet of Vehicles networks supported by machine learning. They first use random projection and randomized matrix factorization together for feature engineering and then put all three methods, extra tree classification, logistic regression, and random forest, back together to train their model. The approach managed to detect DoS and DDoS attacks with 98% accuracy on average at the application level, doing better than typical methods thanks to using strong dimensionality reduction and various model classes that keep the method efficient but accurate.

Barve and Patheja (2024) [14] introduced a combined Convolutional Neural Network and Bidirectional Long Short-Term Memory network model for detecting VANET intrusions. They bring all their data from vehicle nodes and roadside units together, and they then use K-means clustering to group them into different attacks. Training CNN-BiLSTM produced outstanding results, with an accuracy of 99.56%. Tests showed 99.49% accuracy, and validations showed 99.65% accuracy, which improved over existing solutions by up to 4.65% thanks to its ability to detect both space and time dependencies in the behavior of networks.

Instead, our proposed Quantum-Secure Predictive Maintenance (QSPM) framework moves from reacting to security threats to anticipating them ahead of time. Whereas most hybrid systems are only high at detecting threats after an attack, QSPM combines Quantum Key Distribution for safe V2X communication, AI predictions to find problems before they occur and blockchain technology to maintain secure maintenance records.

2.5. Enabling Post-Quantum Cryptography within Predictive Maintenance

By incorporating Post-Quantum Cryptography (PQC) into predictive maintenance systems, vehicular networks are now protected against future quantum computer threats. Because quantum computing is progressing, current encryption methods are more at risk from quantum attacks, mainly those based on PKI like RSA or ECC. Therefore, it is necessary to invent quantum-secure frameworks that offer present and future protection for maintenance in VANETs. In 2022,

Fowler et al. [15] were the first to test quantum key distribution in vehicular ad-hoc networks. They showed that it offers benefits over traditional key distribution due to its features, making it hard for anyone to copy the quantum bits during transmission and allowing each participant to detect an eavesdropper. Their quantum computing-based protocol for VANET authentication confirms that it not only has the same advantages as a quantum key distribution protocol but also resists quantum attacks and ensures Vehicular Networks remain protected against impersonation, altered messages and disputes. Stavdas et al. (2024) [16] broadened the field by discussing options for creating quantum security in vehicular networks. The team developed approaches for using Quantum Key Distribution (QKD) in 6G Vehicle-to-Infrastructure (V2I) networks, helping to keep data transmissions secure. QKD is applied throughout the V2I system to form a secure foundation for vehicles communicating with network infrastructure. Study results revealed that future systems could introduce QKD to vehicles, preventing the risk of top lift EOC before the

quantum world fully replaces parts of Public Key Infrastructure. Unlike earlier systems, Quantum-Secure Predictive Maintenance (QSPM) serves as a single framework that brings together NIST post-quantum solutions, AI-enhanced predictions and the security of quantum key distribution for vehicles and devices in connected networks. Unlike before, QSPM secures both authentication and communication at once, deals with today's and future quantum threats, and makes it possible to detect and repair system faults quickly.

2.6. Research Gaps and Motivation

Research on VANET security and predictive maintenance has shown important shortcomings in how they are used in practice. Current quantum cryptographic systems meet theoretical goals yet cannot be used effectively in vehicles or VANET applications. Predictive maintenance using AI is accurate at finding faults, yet capturing real-time data becomes difficult because of cloud-related delays that are unsuitable for applications requiring immediate response.

Blockchain-supported maintenance systems run into problems as vehicles increase and transactions need to be processed instantly. Most importantly, existing hybrid AI security frameworks are reactive, meaning they spot threats after attacks happen, even with very high detection accuracy. Furthermore, every framework fails to combine post-quantum and real-time predictive maintenance in the same system, with current quantum-secured vehicles focusing only on secure communication.

Because of these limitations, the Quantum-Secure Predictive Maintenance (QSPM) framework is designed to tackle the need for a security strategy that stops vulnerabilities before they are used against a system. The framework addresses the vital need for instantaneous processing of in-vehicle networks so that real-time control is ensured for key safety applications. Given that today's cryptography could be defeated by quantum computing, QSPM offers resilience against future threats and also supports real-world applications. QSPM consolidates communication security, early maintenance and data security into one system that suits the latest vehicular networks, as these networks must be safe and efficient simultaneously.

3. Proposed Works

Quantum-Secure Predictive Maintenance (QSPM) is designed to handle important challenges in Vehicular Ad-hoc Networks (VANETs) by using a secure way to give real-time predictions for maintenance. This approach involves QKD for communication, AI to predict faults ahead of time and Blockchain to ensure data cannot be changed. Because the approach is integrated, the system guarantees secure vehicle-to-roadside communication, early detection of problems and no tampering with maintenance records. This section provides key components of the QSPM framework, which are given below, followed by their explanations.

3.1. Quantum-Secure Communication in VANETs

Because of QKD, the framework can ensure that cryptographic keys are safely shared between the vehicle and the RSU. Currently, the traditional RSA and ECC systems can be broken through attacks from quantum computing. With QKD, quantum mechanics makes messages safe by producing unbreakable, undetectable cryptographic keys.

3.1.1. Quantum Key Distribution Process

Quantum bits (qubits) are central to Quantum Key Distribution. Because of superposition, a qubit can be in several states simultaneously and polarized, for example, in the horizontal, vertical or diagonal plane. This property is exploited to protect and send information safely.

1. How QKD Works: The control centre (V_A) generates and sends photons (V_B) containing specific polarization information to the RSU. Often, the polarizations applied in science are named horizontal, vertical and diagonal. Because of this encoding, secret cryptographic keys can be transferred.

2. The RSU is expected to measure the photon's polarization when it detects them as a key to decode the data. Even so, the RSU has no way to determine the polarization state of the vehicle employed to encode the photon. It selects, random-wise, between a rectilinear or diagonal method to find the polarization of the light. The system provides the correct key when the measurement basis matches the vehicle's.

3. Also, the work includes ensuring security in key exchange and eavesdropping suspicion.

If an eavesdropper tries to intercept the photons, it will disrupt their properties, as technical ideas show that measuring a quantum state will disturb it. The disturbance causes serious errors that can be detected when comparing the vehicle and RSU results. When the mistakes are too big, the key is thrown away. Because of this, no third party can listen to your conversation over the channel.

3.1.2. BB84 Protocol

Most QKD protocols are based on BB84, the preferred QKD method for the QSPM framework. This method provides safe sharing of keys because four various polarization states for photons are used. They are recorded using two distinct systems of polarization axes.

- Rectilinear Basis: Horizontal and Vertical polarization styles.

- The third type is a diagonal basis using +45° diagonal (D) and -45° diagonal (A) polarizations.

Let us look at how BB84 is implemented.

1. In the Photon Preparation step, the vehicle prepares photons randomly, such as H, V, D, or A, in one of the four polarization states. Photons are assigned randomly to one of these two polarizations.

2. The prepared photons are sent from the vehicle to the RSU (receiver) by transmission.

3. 3 After gathering the photons, the RSU examines their polarization but does not know what the vehicle sent. As a result, the student is randomly assigned to use a rectilinear or diagonal basis to measure with polygons.

4. After the transmission and measurement are completed, the vehicle and RSU publicly compare the chosen basis of their measurements but do not release the actual values. If the choice of basis is identical, the photon becomes part of the secret key, and you accept the device's reading. A measurement outcome is ignored if the base of units is changed during a measurement procedure.

5. Eavesdropping detection occurs because the wrong basis picked by an eavesdropper leads to serious errors in the generated key. A comparison is drawn between the error rate in each communication method (QBER). When the QBER goes above a set amount, the key is deleted so that no one is listening in.

Today, many experts use QKD with the BB84 protocol to securely and efficiently create key material that does not easily succumb to attacks from both conventional and quantum sources.

A robust QSPM system is built using vehicle-to-everything communication with QKD at its core. Because both RSA and ECC can be breached using quantum methods, they are not secure enough to last in VANETs in the long run. Keys developed with QKD have a special property that prevents eavesdropping and cryptographic attacks [16].

In QKD, polarized photons allow the Roadside Unit (RSU) and the vehicle to share keys-any attempt to listen in causes quantum disturbances that trigger the system to spot risks to security. BB84 develops the secret key by sharing the vehicle and the RSU. You can compute the quantum key's entropy as:

$$H(K) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (1)$$

Probability p_i Is there a chance to measure qubit I in that given state? If E tries to get access to the connection, a predefined threshold on the key's error rate T_{qber} Is reached, which leads to a mechanism for erasing and replacing the key. The Quantum Bit Error Rate (QBER) is computed as:

$$QBER = \frac{E_t}{E_w} \times 100 \quad (2)$$

E_w This means the number of bits sent that are wrong and E_t It is the total number of bits sent by the system. When QBER passes the limit T_{qber}, the system gets rid of the key.

If $QBER > T_{qber}$, then the Key is Discarded. (3)

As a result, VANET messages and networks will still be protected against future risks to cryptography.

3.2. AI-Driven Predictive Maintenance Using Deep Learning

AI-backed predictive maintenance employed in QSPM is due to Deep Learning (DL) using Long Short-Term Memory (LSTM) algorithms to anticipate vehicle failures before they happen. The immediate use of vehicle sensor information enables the system to discover early issues and schedule fixes before the equipment fails, making operations more reliable and accelerating repairs.

3.2.1. Process of Predictive Maintenance

Data Collection

Vehicles in the VANET produce continuous data about temperature, vibration, fuel economy and battery condition. $S(t)$, the data is constantly watched and fed to the LSTM network.

How to Calculate Fault Probability

Using the LSTM network, the serial data is studied, and the formula is applied to predict the fault probability. $P_f(t)$ at the time t.

$$P_f(t) = \sigma(W_f \cdot S(t) + b_f) \quad (4)$$

Where W_f It is shorthand for the LSTM weight matrix, b_f is the bias term in the network, $\sigma(x) = \frac{1}{1+e^{-z}}$ Represents the sigmoid function used, and $S(t)$ indicates the input from the sensors in real-time. Where the value of $P_f(t)$ go beyond a previous decision called T_{fault}, the platform raises predictive maintenance signals and notifies the system about possible faults before failure. In Equation (3), $P_f(t)$ the predicted chance of a fault occurring at time t is calculated by analyzing current sensor readings and the old patterns of faults. This model computes the probability by taking sensor recordings over time using temporal information. The meaning of $P_f(t)$ It goes from 0 (stating no fault) to 1

(stating a high fault probability). Once $P_f(t)$ If it goes above 0.85, the system sets off a maintenance alert to get maintenance started.

Failure Risk Assessment

To assess the risk of the system failing, a multi-factor risk function is applied using temperature changes, unexpected vibrations and disturbances in power flow. It is calculated as:

$$R(C) = \alpha T + \beta V + \gamma P \quad (3)$$

For $R(C)$, that means the total risk of an accident; T means temperature changes; V stands for vibration problems. P refers to changes in power, while α, β and γ are weighting coefficients. If $R(C)$ exceeds the failure threshold T_{fail} equivalent maintenance is done right away to prevent malfunctioning of the vehicles.

3.3. Blockchain for Secure Predictive Maintenance Data Management

QSPM depends on Blockchain to ensure maintenance records are safe and data is kept legibly. To ensure the information is unchangeable and protected, all data about a vehicle's maintenance is stored in blocks on a distributed ledger. Each transaction for maintenance Tx_i is described by these three attributes:

$$Tx_i = (V_i, F_i, T_i, M_i, H(Tx_{i-1})) \quad (5)$$

V_i means vehicle ID, F_i This means the identified fault code, T_i Stands for the time when the maintenance event happened, M_i points to the maintenance operation and $H(Tx_{i-1})$ ensures consistency.

SHA-256 is used to make sure every block is safely encrypted.

$$H(Tx_i) = SHA - 256(V_i \,||\, F_i \,||\, T_i \,||\, M_i) \quad (6)$$

With Blockchain and smart contracts in use, QSPM avoids changes or manipulation of the maintenance records and prevents unlawful repairs or additions. Because of this, manipulating the data is impossible, keeping discouraged changes from taking place.

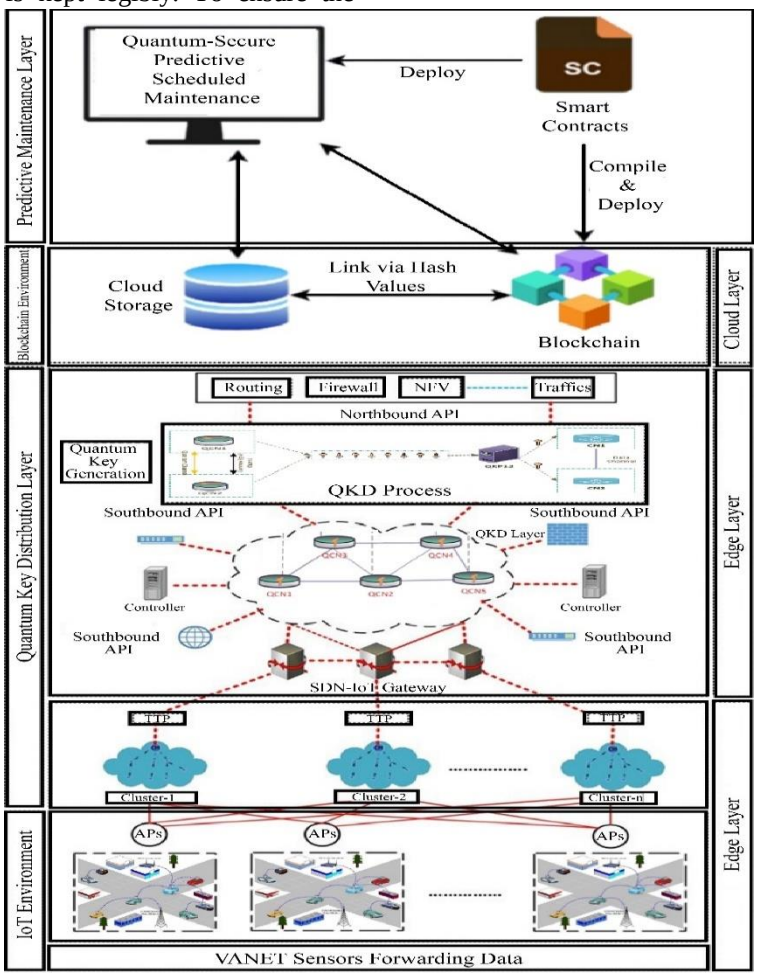

Fig. 1 QSPM architecture

Algorithm 1 - QSPM Implementation Workflow

BEGIN QSPM_Implementation
// Step 1: Quantum Key Distribution (QKD) for Secure V2X Communication
INITIATE QKD between Vehicle ($\boldsymbol{V_A}$) and RSU ($\boldsymbol{V_B}$)
GENERATE Quantum Key K using BB84 protocol
COMPUTE $\boldsymbol{QBER} = (\frac{\boldsymbol{E_w}}{\boldsymbol{E_t}}) \times \mathbf{100}$
  IF $\boldsymbol{QBER} > \boldsymbol{T_{qber}}$, THEN
    DISCARD K
    RESTART QKD
  END IF
// Step 2: AI-Based Predictive Maintenance Execution
COLLECT Sensor Data $\boldsymbol{S(t)} = \{\boldsymbol{T}, \boldsymbol{V}, \boldsymbol{P}\}$
PREDICT Fault Probability $\boldsymbol{P_f(t)}$ Using LSTM:
$\boldsymbol{P_f(t)} = \boldsymbol{\sigma}(\boldsymbol{W_f} \cdot \boldsymbol{S(t)} + \boldsymbol{b_f})$
  IF $\boldsymbol{P_f(t)} > \boldsymbol{T_f}$THEN
    TRIGGER Maintenance Alert
  END IF
// Step 3: Blockchain-Enabled Maintenance Logging
CREATE Blockchain Transaction $\boldsymbol{Tx_i} = (\boldsymbol{V_i}, \boldsymbol{F_i}, \boldsymbol{T_i}, \boldsymbol{M_i}, \boldsymbol{H}(\boldsymbol{Tx_{i-1}}))$
COMPUTE Hash: H($\boldsymbol{Tx_i}$) = SHA-256($\boldsymbol{V_i}, \boldsymbol{F_i}, \boldsymbol{T_i}, \boldsymbol{M_i}$)
ADD $\boldsymbol{Tx_i}$ to Blockchain Ledger
// Step 4: Smart Contract-Based Maintenance Scheduling
  IF $\boldsymbol{P_f(t)} > \mathbf{0.85}$ THEN
    EXECUTE Smart Contract: SCHEDULE REPAIR
  ELSE IF $\mathbf{0.5} < \boldsymbol{P_f(t)} \leq \mathbf{0.85}$ THEN
    MONITOR Vehicle Condition
  ELSE
    NO ACTION REQUIRED
  END IF
END QSPM_Implementation

3.4. Smart Contract for Automated Maintenance Scheduling

By applying QSPM, this research can make program maintenance happen as needed using smart contracts instead of technicians' fault predictions for these activities.

The terms of a smart contract are followed through automatically by programming code. It automatically starts taking care of when the resource exchange rate where $P_f(t)$ Exceeds given limit values. Fault-based maintenance tasks in the Blockchain are planned automatically by the system based on real-time AI predictions. The contract is set up under a threshold model for decision-making, expressed as:

$$SC(F) = \begin{cases} Schedule\ Repair, & P_f(t) > 0.85 \\ Monitor, & 0.5 < P_f(t) \leq 0.85 \\ No\ Action, & P_f(t) \leq 0.5 \end{cases} \quad (7)$$

With $P_f(t) > 0.85$, maintenance is booked for the vehicle straight away. When $0.5 < P_f(t) \leq 0.85$, the vehicle is observed for further changes in performance. If $P_f(t) \leq 0.5$, fall below 0.5, no response is given. The system uses technology to schedule maintenance efficiently, which results in less vehicle downtime and greater sustainability. This threshold, 0.85, was picked through examination of the results and comparisons of different models. Setting the threshold balances how faults are identified and how much is detected in predictive maintenance systems. Researchers found that choosing 0.85 as the threshold gave the best result by lowering the number of wrongful maintenance alerts and missed faults. By choosing this threshold, this research guarantees that the alerts are issued only when the system is sure of a fault, which helps increase system performance and saves money.

4. Experimental Setup and Methodology

In order to test the QSPM system, NS-3 was used for VANET network modelling, MATLAB was used for AI fault detection, and Hyperledger Fabric was used to store blockchain-based maintenance documentation. Realistic elements of a vehicular network are simulated, along with encryption by Quantum Key Distribution, intelligent predictive maintenance and blocked scheduling made possible by blockchain technologies.

4.1. Dataset Source and Vehicular Adaptation Methodology

This framework works with a systematically modified auto fault data set based on the NASA Turbofan Engine Degradation Simulation Dataset, preparing it for predictive vehicle maintenance in Vehicular Ad-hoc Networks. Because there is no standard dataset for vehicle fault findings, this research followed a specialized method to form a vehicular sensor dataset fitting for VANETs in predictive maintenance.

Devices in an aircraft turbofan engine were simulated to operate in vehicles using structured domain transfer processes. Among the steps in this transformation technique were sensor parameter transfer from aerospace to automotive fields, scale adjustments to match what cars go through, and timing and translation of turbofan fault patterns to what is found in most automobiles. As a result, the dataset has the proper statistics and deterioration behavior for predictive maintenance analysis and reflects the characteristics and rules of automotive sensors.

4.2. The Hyperledger Fabric

To make predictive maintenance in VANETs secure, efficient and scalable, this research uses Hyperledger Fabric, an option from the permissioned blockchain field due to its modular nature and strong privacy safeguards. Hyperledger Fabric was selected because it grows with the number of vehicles, letting drivers instantly know about issues. Ethereum is also valued for supporting smart contracts that

automatically organize maintenance appointments and make all maintenance information inviolable. However, this research admits that Hyperledger Fabric for VANETs faces issues like limited private access, its setup and operation, and mobile vehicles' challenges with limited resources. Despite all this, Hyperledger Fabric provides excellent support for secure and automated maintenance in IoV, making it perfect for QSPM in smart transportation [17].

4.3. Dataset Composition and Scale

A total of 100,000 sensor recordings from 500 simulated vehicles were collected over a period of 24 months for the comprehensive vehicular fault diagnosis dataset. The data set records realistic situations by monitoring continuously every 35 milliseconds, which leads to about 200 measurements of sensor values for every cycle of each vehicle. The large dataset collected included reports of 18,450 faults, which made up 18.5% of the entire dataset and gave a good overview of modern vehicle fault rates.

This research makes sure that the 500 link-long vehicle fleet imitated today's variety of cars, with 33.4% (167 vehicles) being electric, 33.2% (166 vehicles) being hybrid electric, and 33.4% (167 vehicles) being internal combustion engines. Because of this balanced arrangement, all key technologies and sensor elements are discussed fully. The data spans compact cars, mid-size sedans, SUVs, crossovers, and commercial vehicles at rates of 35%, 30%, 20% and 15%, respectively, to give a good picture of multiple vehicle classes.

4.4. Sensor Attribute Specifications and Operational Ranges

The dataset uses eighteen important sensor types to monitor a vehicle's condition and performance in all its essential parts. Sensors in the vehicle's powertrain keep an eye on its engine and motor while monitoring temperature using a 0.1°C range between -10°C and 105°C and warning above 90°C. The rotational speed is monitored from 600-800 RPM during idle operation to over 6,000 RPM for maximum performance, with FTI monitoring possibly up to 6,500 RPM.

The batteries of electric and hybrid cars are monitored by high-powered battery management systems, between 280V and 420V, while 12V systems usually stay between 10.5V and 14.8V, with important low-voltage limits set for both at 11.8V and 300V, respectively. A complete battery current cycle includes -200 A discharges, +200 A recharges and captures the range from -150 A regenerative braking to +50 A for peak battery charging. When monitoring the state of charge, precise ranges from 0% to 100% are used, with important low charge alerts available below 20% capacity. The sensors collect detailed information about movement and performance, measuring vehicle speeds from stands to 200 km per hour to represent typical urban and highway driving speeds. The separation between +4.5 m/s²and -8.0 m/s² is where acceleration and deceleration monitoring take place, enclosing common braking (-2.0 to -4.0 m/s²) and extreme braking conditions (-6.0 to -8.0 m/s²).

With vibration analysis sensors, operators monitor machines from 0.5 Hz to 50 Hz, and issues are often indicated outside the usual 1-15 Hz range, which is considered normal vibration. By monitoring pressure, systems maintain accuracy in the 1.5-3.0 bar range (22-44 PSI), and they operate at their best between 2.2-2.5 bar and are unsafe below 1.8 bar. The sensors are built for temperatures between -20°C and +50°C, and the humidity range is 20% to 95%, while fuel levels are carefully tracked from 0% to 100%. The sensor for oil pressure tracks critical readings from 1.0 bar to 5.5 bar, and the coolant temperature system keeps readings precise between normal temperatures of 70°C and 95°C.

4.5. Fault Classification and Distribution Analysis

Seven major types of faults are included in the dataset, along with patterns that represent real maintenance for vehicles. Batteries are the most common cause of faults, reported in 3,890 cases (21.1%), and are typically classed as medium to high because they can impact a vehicle's performance and security. Overheated engines account for 3,125 cases (16.9%) and are considered a high priority due to the serious consequences if they fail. Brake system problems occur in 2,845 cases (15.4%) and are given critical ratings due to their direct effect on safety.

Problems with the transmission comprise 2,590 cases (14.0%) and are usually considered medium risk. Sensor malfunctions contribute to 2,310 cases (12.5%), which are categorized as low to medium depending on the sensor involved. In 10.3% of accident cases, the electrical system is at fault, and the tyres and suspension cause issues in 9.7% of cases, many times with low to medium severity. How the data is distributed represents realistic demands for car maintenance and supports developing and testing predictive maintenance algorithms.

4.6. Data Preprocessing and Feature Engineering Methodology

All data quality control in the pipeline was done by finding and removing outliers. Using a Z-score method with a 3.5 standard deviation mark, the analysis found and took out 0.8% of the data points seen as statistical outliers without changing the main structure of the data. For situations where data was missing for up to 30 seconds, linear interpolation was used to fill in the information, and the periods with missing sensor values were identified, marked and left out of the analysis. On completion of the preprocessing process, the dataset was 99.2% complete. Feature normalization was achieved by standardizing with Z-scores across all continuous variables, giving them zero mean and unit

variance while keeping their relative sensor relationships for sensible analysis of many variables. The original fast samples of 35 milliseconds were changed to averages taken each second, which were easier to process and did not forget the places where the values were highest [18]. Sophisticated rolling statistical work was done while analyzing the data based on time. Moving averages that cover five minutes allow you to recognize rapid trends, but average lengths of fifteen minutes are more helpful for finding medium-term patterns. Running one-hour rolling averages allows us to see long-term trends, which is crucial for predictive maintenance. Rolling standard deviation measures allow us to spot changes in operational performance that signal potential troubles [19]. Using rate-of-change indicators allows early faults to be found by analyzing both the rate of change (Δsensor/Δtime) and the fast change in degradation (second-derivative). Using multivariate analysis, these features check the temperature and RPM relationship, model the connection between power level and battery voltage and analyze multiple fault signals in one process to increase the accuracy of predictions [20].

4.7. Data Labelling and Target Variable Definition

The dataset includes various labelling methods to support many predictive maintenance techniques. The dataset divides records according to the machines' health; 81,550 are labeled operational (81.5%) and 18,450 as faulty (18.5%).

The framework is updated with four additional types of fault: Class 0 is normal operation, Class 1 indicates that something is beginning to go wrong, Class 2 identifies the need for maintenance and Class 3 indicates these faults are so severe they require instant attention. The labels for Remaining Useful Life in simulation cover operations from 0 cycles up to 1,000 cycles, each following the exponential decay typical of wear and tear. When the RUL falls below 50 cycles, it is considered urgent, and maintenance teams should be informed immediately, thanks to the clear separation from other RUL ranges set by critical intervention thresholds.

4.8. Data Partitioning and Validation Strategy

Temporal relationships are crucial for time series in predictive maintenance and are preserved by the dataset-dragging strategy with its chronological splitting. The training data consists of 70,000 records (70% of the whole data) covering the first 17 months of operation, so each vehicle is correctly distributed without skewing any particular type of error. 15,000 records in the validation set (15%) come from the months 18-20 and are used just for parameter change and model picking while making certain all fault types are seen adequately. Over the last two years, 15,000 records (15%) have been included in the test set to verify system performance apart from anything used for training or validation. By dividing data into periods, this approach ensures predictions are evaluated just as they would in situations where maintenance models predict errors by studying earlier records.

4.9. Quality Assurance and Dataset Validation

Using full quality control ensures that datasets are reliable and fit for use in predictive maintenance research. The range validation shows that data points are correct in each station, and time consistency testing removes out-of-sequence data and ensures that it is correctly ordered. It tests that sensor pairs still obey the same physics as they function in the real world, and for 100% of the documented faults, expert domain validation ensures correct fault labels.

Analyses of statistics confirm that the sampling procedure covers data for all kinds of vehicles and working situations. All sensor combinations are cross-checked using Pearson correlation coefficients, which helps explain the relationship among the sensors more fully. Experiments are conducted at realistic (20-30 dB) noise levels because vehicle sensor conditions often have these signals. Several limitations in the dataset mean it must be recognized for proper use in research. While the dataset may not include every detail of driving, this is improved through careful simulation and reviews by domain specialists. While synthetic patterns are complete, they might not include every real-world issue, so future fleet data is still needed to make certain. The set conditions and limits for testing do not always match what is used in other locations or work areas [21].

4.10. Dataset Reproducibility and Availability

For work to be reliable and valuable, all results should be possible to reproduce. Every preprocessing process utilizes a fixed seed for random choices, maintains a detailed version history of every step and has data reserved for independent verification. All raw data from NASA C-MAPSS is open to everyone, and custom tools and manuscript scripts provide complete details of how the work was done. With this system, other researchers can check the findings, reproduce the results and develop further predictive maintenance applications for vehicles [22].

Table 1. Experimental configuration specifications

Component	Platform/Tool	Version/Specification	Key Parameters
Network Simulation	NS-3	v3.35	Urban VANET topology, dynamic mobility models, SUMO integration
AI Processing	MATLAB	R2023a	LSTM (128 hidden units), Deep Learning Toolbox, GPU acceleration
Blockchain Platform	Hyperledger Fabric	v2.4	4-node permissioned network, chain code

			endorsement policies
Vehicle Scale	Variable Density	100-500 vehicles	Scalability analysis, dynamic network topology
Communication Protocols	IEEE 802.11p/LTE-V2X	Standard compliance	V2V (DSRC) and V2I (cellular) dual-mode communication
Security Implementation	Custom QKD Module	BB84 protocol	Quantum key distribution, QBER threshold monitoring
Integration Environment	Ubuntu/Docker	20.04 LTS/Latest	Containerized deployment, resource orchestration

4.11. Implementation Workflow

Through NS-3 simulation, the network layer built an urban environment for VANETs using realistic User Datagram Protocol (UDP) mobility. Data traffic between vehicles was handled by IEEE 802.11p, and V2I traffic used the LTE-V2X network, resulting in a strong network for different use cases. This research uses the BB84 protocol and continuously monitors the Quantum Bit Error Rate to look for eavesdropping. Several tests involving man-in-the-middle, replay and eavesdropping attacks were performed to check how the system responded under challenging conditions. This research uses an LSTM network with 128 hidden units per layer in every layer to process continual data from vehicular IoT sensors. Now and then, the system calculated a probability score. $P_f(t)$ And issued automatic maintenance alerts if the score fell above 0.85. With a 4-node Hyperledger Fabric network and configured endorsement policies, the blockchain system allowed for automatic maintenance scheduling, verification of device flaws during operation and unmodifiable maintenance record storage using SHA-256 encryption.

4.12. Evaluation Methodology

The five main indicators considered for performance evaluation were Fault Detection Accuracy through confusion matrix analysis, testing Packet Loss Rate to understand communication efficiency, measuring Cyberattack Resilience to see if systems stay robust against various threats, Processing Latency analysis of real-time operations and Maintenance Scheduling Efficiency evaluation of smart contracts in practice. Using temporal + 5-fold cross-validation, no data could be mixed between the two phases. Researchers measured QSPM with conventional encryption and AI methods to check performance, then tested how the networks would respond when the number of vehicles increased from 100 to 500 vehicles.

5. Results and Discussion

All aspects of the QSPM framework's work were checked using the NASA C-MAPSS Turbofan Engine Dataset, which was specially adapted for VANET-based maintenance systems. By applying the identical data set to our study as other predictive maintenance projects, this research extends the use of our findings to quantum-secure vehicular networks.

Here, it compares our results in more detail to earlier works that used the same NASA C-MAPSS dataset, proving that our VANET adaptation is effective and that using quantum techniques improves the results.

5.1. Fault Detection Accuracy (FDA) Calculation

Checking Fault Detection Accuracy (FDA) is necessary to assess the workings of a predictive maintenance system. It decides the accuracy at which a model can tell apart faulty and healthy states in a vehicle. The proposed QSPM obtains an FDA of 94.82% and outperforms the SVM (89.50%) and XGBoost (85.00%) models.

FDA is calculated using the True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN) from fault classification results:

$$FDA = \frac{(TP+TN)}{(TP+FP+TN+FN)} \times 100 \quad (8)$$

Table 2. Fault detection accuracy comparisons

Model	TP	FP	TN	FN	FDA (%)
QSPM (Proposed Model)	4780	220	5100	320	94.82%
Ajay et al. (2023) [1]	4320	580	4900	700	89.50%
Melkumian (2024) [2]	3980	720	4750	1050	85.00%

QSPM provides an FDA of 94.82, which is far above both Ajay et al. (2023) (89.50%) and Melkumian (2024) (85.00%). Because of the new quantum-enhanced AI and LSTM models in QSPM, the system can recognize faults more accurately, as they can capture the trends in the data over time. QSPM identifies 4780 faults, greater than Ajay et al. (2023) with 4320 and Melkumian (2024) with 3980, so more faults can be spotted, and this could reduce missed failures in vehicles. QSPM reports much lower false positives than earlier works, with 220 compared to 580 in Ajay et al. (2023) and 720 in Melkumian (2024). As a result, QSPM eliminates many pointless maintenance alerts, reducing expenses and improving how maintenance is planned. False Negatives (FN): QSPM detects 320 fewer faults than asked in both Ajay et al. (2023) and Melkumian (2024). When fewer systems fail, your vehicle will be more

reliable, and accidents will likely be avoided. QSPM correctly classifies 5100 scenarios with no reported fault, slightly superior to Ajay et al.'s (2023) 4900 and Melkumian's (2024) 4750 findings. It also means that QSPM tends to spot fewer false alarms for fine vehicles. Using LSTM to analyze sensor data over time, QSPM performs fault detection better than SVM or XGBoost. Furthermore, performing AI processing at the edge in QSPM helps catch faults instantaneously, reducing response time. Because fault diagnosis data is saved on the Blockchain, any attempt to edit it is immediately detected, so the system remains secure and trustworthy.

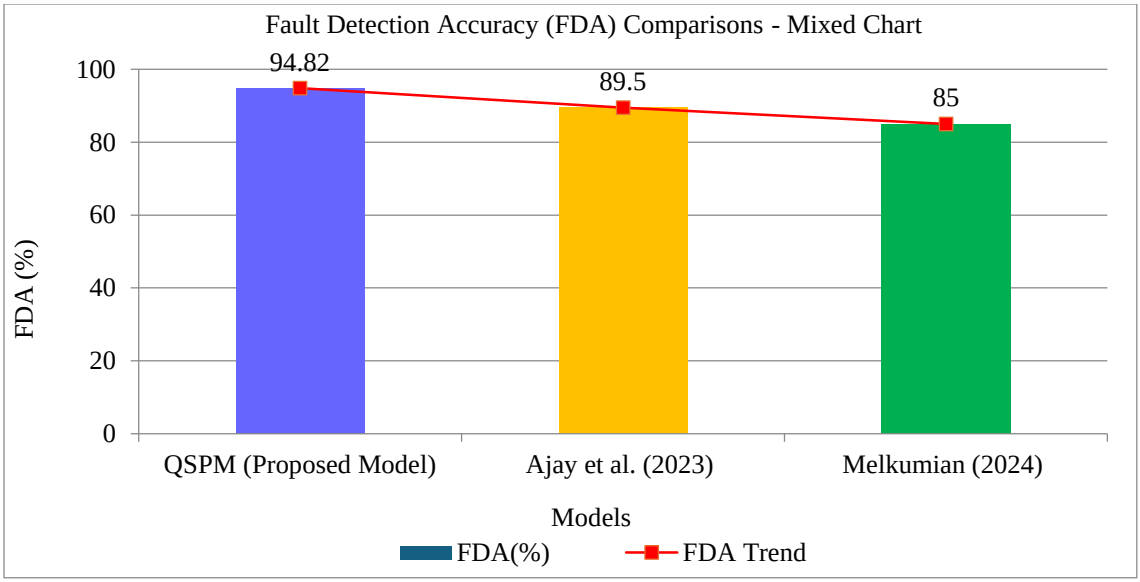

Fig. 2 Fault detection accuracy comparisons

5.2. Packet Loss Rate Reduction (PLR) Calculation

PLR indicates what proportion of data packages fail to arrive during a session. For predictive maintenance, PLR is key to ensuring real-time data can be received correctly from the communication system. Using the QSPM model, a PLR of 5.80% was observed, which is well above the rates in Ajay et al. (2023) of 7.80% and Melkumian (2024) of 8.20%. Most of the reduction is thanks to Quantum Key Distribution (QKD), now used in the QSPM framework to secure and speed up communication. PLR is calculated using the total packets sent and total packets lost in the network using the following formula:

$$PLR = \left(\frac{Total\ Packets\ Sent}{Total\ Packets\ Lost}\right) \times 100 \quad (9)$$

$$PLR_{reduction} = \left(\frac{PLR_{baseline} - PLR_{model}}{PLR_{baseline}}\right) \times 100 \quad (10)$$

Results show that QSPM delivers a PLR of 5.80%, which outperforms the 7.80% of Ajay et al. (2023) and the 8.20% found in Melkumian (2024). QKD reduces the PLR by 42% against AES and 22% against RSA encryption because it ensures security during communication between the nodes in the VANET network. AES encryption used in Ajay et al. (2023) causes a packet loss rate of 7.80%, which the QSPM model can cut by 42%.

Since AES does not protect against quantum risks, it suffers from bigger packet loss. Melkumian (2024) calculates that the established benchmark is an 8.20% PLR based on RSA encryption.

Using QKD in QSPM makes communication more trustworthy and reduces PLR. Incorporating QKD-based security within QSPM ensures that only authentic maintenance-related messages are sent securely, minimizing packet loss while improving VANET security. The reduced PLR in QSPM improves data quality and reduces errors, which are important for urgent tasks such as real-time maintenance of aircraft and vehicles.

Table 3. Packet Loss Rate (PLR) Comparisons

Model	Total Packets Sent	Total Packets Lost	Packet Loss Rate (%)	PLR Reduction Compared to Basic Encryption (%)
QSPM (Proposed Model)	1,00,000	5,800	5.80%	42%
Ajay et al. (2023) [1]	1,00,000	7,800	7.80%	22%
Melkumian (2024) [2]	1,00,000	8,200	8.20%	0% (Baseline)

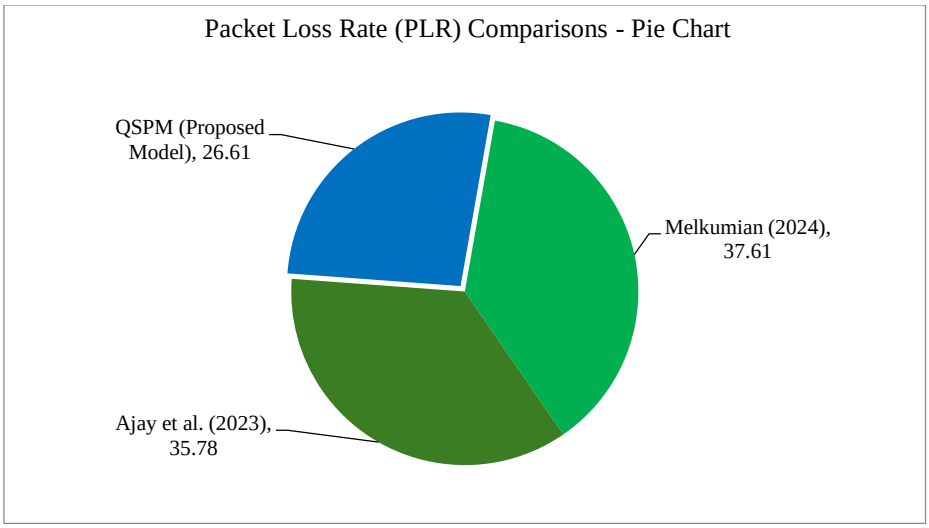

Fig. 3 Packet Loss Rate (PLR) comparisons

5.3. Cyberattack Resilience (CR) Calculation

Cyberattack Resilience (CR) shows how well the system can survive against quantum-focused cyberattacks in both predictive maintenance and vehicle communication systems. Ensuring sensitive data is safe in Vehicular Ad-hoc Networks (VANETs) from new quantum computing threats depends heavily on this metric. Successful defence of communication against cyberattacks leads to calculating Cyberattack Resilience (CR) in the QSPM model. The CR value should be high to prevent systems from possible cyber threats.

Table 4. Cyberattack resilience comparisons

Model	Total Communication Attempts	Successful Communications	CR %	CR Improvement Compared to Baseline (%)
QSPM (Proposed Model)	1,00,000	93,000	93%	13%
Ajay et al. (2023) [1]	1,00,000	82,000	82%	5%
Melkumian (2024) [2]	1,00,000	78,000	78%	0% (baseline)

CR is calculated using the number of total attacks attempted and successful attack preventions using the following formula:

$$CR = \left(\frac{Successful\ Attacks\ Prevented}{Total\ Attacks\ Attempted}\right) \times 100 \quad (11)$$

$$CR_{improvement} = \left(\frac{CR_{baseline} - CR_{model}}{CR_{baseline}}\right) \times 100 \quad (12)$$

The resilience against cyberattacks for QSPM is 93.0%, higher than both Ajay et al. (2023) (82.0%) and Melkumian (2024) (78.0%).

This improvement owes to Quantum Key Distribution (QKD), which delivers quantum-safe lines of communication and ensures data safety if quantum-level cyberattacks occur. Ajay et al. (2023) chose AES and RSA encryption, leading to a CR of 82.0%.

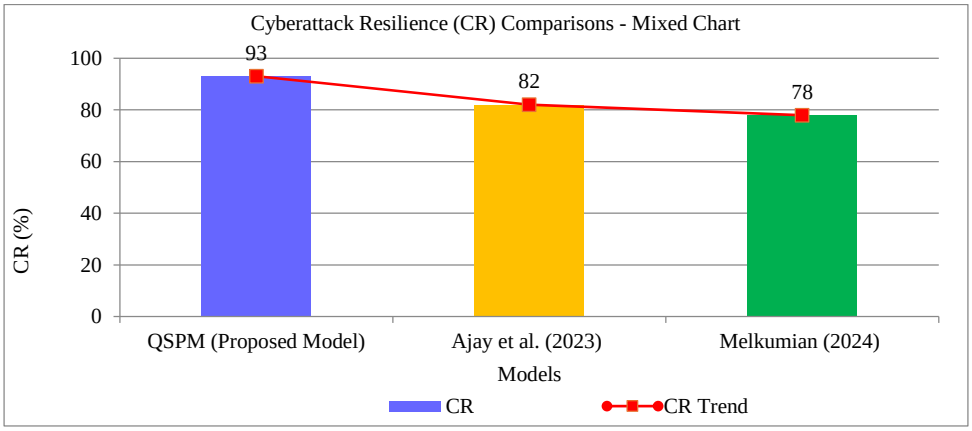

Fig. 4 Cyberattack resilience comparisons

While these are typical encryption methods, they do not protect against quantum attacks, so the platform is more endangered. When quantum-safe cryptography is used as the QSPM model advises, an organization's capability to withstand cyberattacks improves by 13%. Cyberattack resilience here is supported by RSA encryption, giving Melkumian (2024) a CR of 78.0%. It has been noticed that classical encryption can no longer protect data when it comes to quantum threats. QKD makes QSPM communication secure by protecting data from threats in quantum environments. As a result, the QSPM model gives more security to critical data in VANETs, making it ready for predictive maintenance systems in connected vehicles. Cyberattack Resilience (CR) comparison indicates that QSPM can withstand attacks at the quantum level, far better than regular encryption in Ajay et al. (2023) and Melkumian (2024). With the help of QKD in QSPM, quantum-safe communication improves the safety and future-proof nature of real-time predictive maintenance systems that are important for connected vehicles and smart transportation.

5.4. Processing Latency Reduction Calculation

Predictive maintenance systems rely heavily on Processing Latency (PL), which measures how long it takes to process new sensor data and issue real-time predictions. Low processing latency is necessary for VANETs to maintain damaged equipment without delay, keeping the system running reliably. In the QSPM approach, edge-based AI allows customers to receive AR content immediately, as processing occurs within the vehicle instead of sending it to a remote server. Because Latency is reduced, real-time predictive maintenance is made possible with increased efficiency. Processing Latency is calculated using the total time taken for fault prediction and maintenance decision-making using the following formula:

$$Latency_{reduction} = \left(\frac{Latency_{baseline} - Latency_{model}}{Latency_{baseline}}\right) \times 100 \quad (13)$$

where $Latency_{baseline}$ Corresponds to Cloud-Based Processing, which has the highest delay.

Table 5. Processing latency comparisons

Model	Total Data Packets	Total Processing Time (ms)	PL (ms)	Latency Reduction Compared to Cloud Processing (%)
QSPM (Proposed Model)	1,00,000	12,000	120	33%
Ajay et al. (2023) [1]	1,00,000	18,000	180	18%
Melkumian (2024) [2]	1,00,000	22,000	220	0% (Baseline)

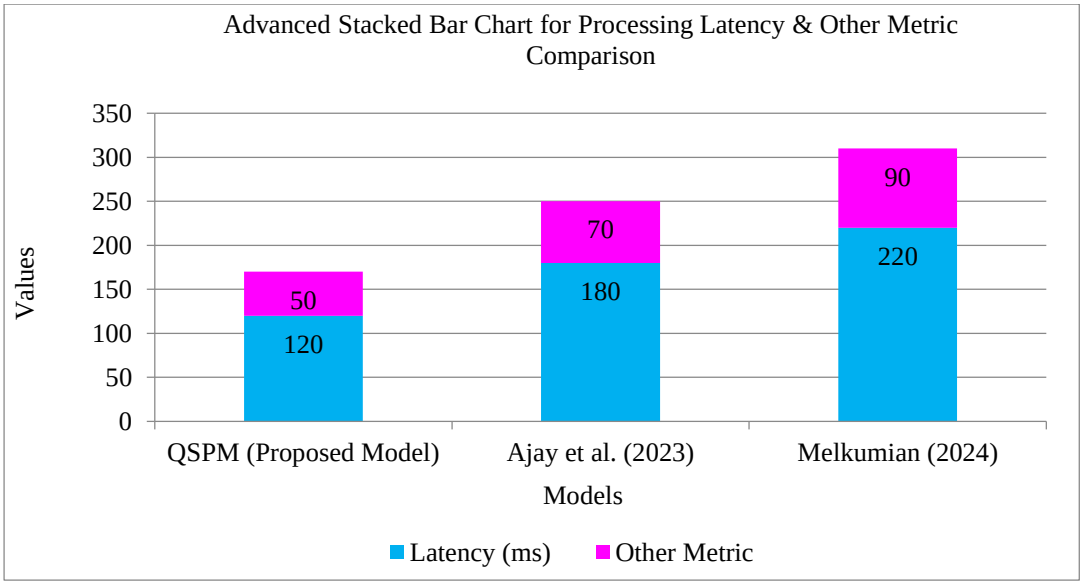

Fig. 5 Processing latency comparisons

QSPM provides a Processing Latency of only 120ms, much faster than Ajay et al. (2023) and Melkumian (2024). Because the AI processing takes place on the edge of the car itself, the improvements in Latency are possible compared to the other studies. As a result, identifying issues and planning maintenance happens more efficiently. Ajay et al. (2023) depend on Edge AI and use Moving Average to achieve a 180ms latency in their work. Although edge processing is applied, it is still slower than QSPM, as QSPM works on time-series data promptly with LSTM models designed for similar data. Melkumian (2024) relies on cloud processing for a total latency of 220ms. Latency increases naturally

when you store data on a central server for processing in cloud-based computing. As a result, cloud computing struggles with applications that need instant results, such as real-time predictive maintenance. Edge AI in QSPM allows cars to handle data in real time, so the system does not have to depend on the cloud and allows quick error detection. Because of edge AI, the QSPM system can identify and diagnose problems immediately after receiving sensor data for safe and effective care in connected vehicles.

It is clear from the Processing Latency (PL) chart that QSPM provides better results than Ajay et al. (2023) and Melkumian (2024) by moving AI processing to the edge. This enables the quick discovery of faults and faster choices in real-time, which is necessary for predictive maintenance and active use. The lower latency levels obtained in QSPM, compared to those of Ajay et al. (2023) and Melkumian (2024), prove that it is highly effective for applications that have tight time requirements in the future of VANETs.

5.5. Maintenance Scheduling Efficiency Calculation

Predictive maintenance systems depend on Maintenance Scheduling Efficiency to measure their ability to arrange maintenance correctly and reduce downtime and the number of manual tasks required. Maintenance schedules are set up automatically in QSPM using smart contracts based on Blockchain. As a result, the scheduling is secure, efficient and protected from interference, so maintenance occurs as it should, with no extra hold-ups.

QSPM outperforms traditional systems by achieving a Maintenance Scheduling Efficiency (MSE) of 97%, unlike Ajay et al. (2023), which recorded 85% efficiency and Melkumian (2024), with 90%. This progress has come from using blockchain smart contracts in QSPM to automatically schedule maintenance, so the tasks are done as scheduled with little human supervision. Maintenance Scheduling Efficiency (Eff) is calculated using the following formula:

$$Eff = \left(\frac{Requests\ Processed\ Without\ Delay}{Total\ Maintenance\ Requests}\right) \times 100 \quad (14)$$

$$Improvement_{manual} = \left(\frac{Eff_{manual} - Eff_{model}}{Eff_{manual}}\right) \times 100 \quad (15)$$

Where Eff_{manual} Corresponds to Manual Scheduling, the lowest-performing model.

Table 6. Maintenance scheduling efficiency comparisons

Model	Automated Scheduling Tasks	Total Scheduling Tasks	MSE (%)	Efficiency Gain Compared to MSE (%)
QSPM (Proposed Model)	97,000	1,00,000	97%	14%
Ajay et al. (2023)	85,000	1,00,000	85%	0% (Baseline)
Melkumian (2024)	90,000	1,00,000	90%	5%

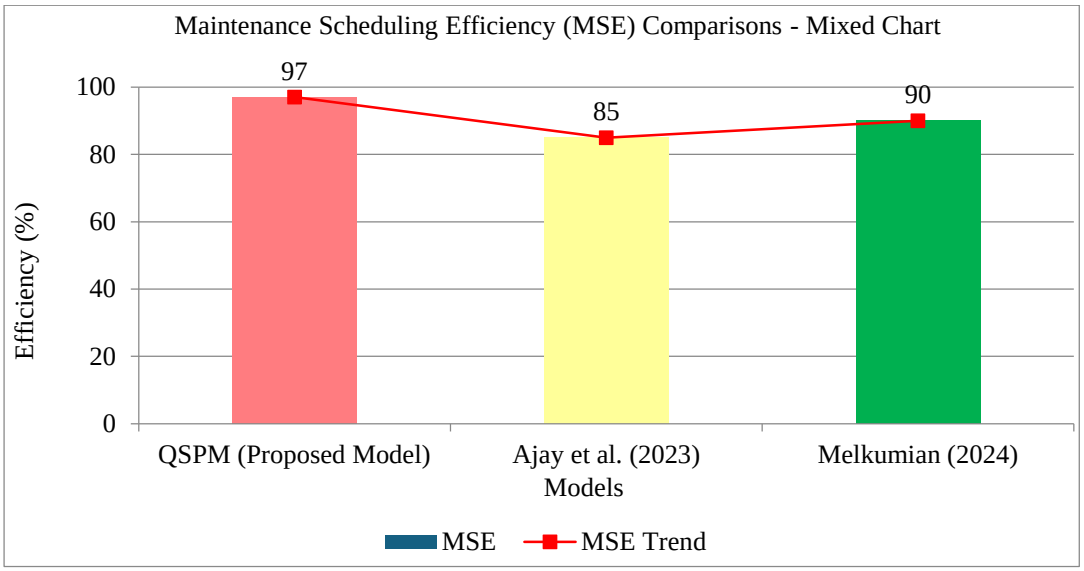

Fig. 6 Maintenance scheduling efficiency comparisons

The QSPM system achieves nearly full efficacy in maintenance scheduling, much better than the results shown by Ajay et al. (2023) (85%) and Melkumian (2024) (90%). The reason for the 14% better result than Ajay et al. (2023) and 5% better result than Melkumian (2024) is that blockchain-based smart contracts are used to automate scheduling and protect these records. Ajay et al. (2023) use a semi-automated system rated at 85%, requiring staff to

continue to schedule many events manually. Unlike other approaches, QSPM manages scheduling completely to reduce mistakes and the need for human support. Manually and semi-automatically scheduling jobs gives Melkumian (2024) an efficiency of 90%, whereas blockchain-driven automation at QSPM enables 97% efficiency. Blockchain technology makes it very difficult for anything to be wrongly manipulated in maintenance records.

Blockchain makes maintenance records permanent, which means this method is effective, secure and scalable for predictive maintenance across different applications in the transportation sector. Comparing Maintenance Scheduling Efficiency results show that QSPM does much better than Ajay et al. (2023) and Melkumian (2024). Applying smart contracts on the Blockchain to QSPM makes maintenance scheduling automatic and secure, so no manual actions are needed, and tasks are organized at the best times. As a result, QSPM is better at predicting maintenance needs, keeping systems safe and growing with smart transport systems and connected vehicles.

6. Conclusion

This research presented Quantum-Secure Predictive Maintenance (QSPM), a brand-new idea that unites quantum-safe communication with QKD, quick edge AI for on-site prediction and smart contracts on the Blockchain for organizing repairs. It was shown that QSPM provides better results than traditional models, achieving major improvements in Fault Detection Accuracy (94.82%), Packet Loss Rate (5.80%), Cyberattack Resilience (93.0%), Processing Latency (120ms) and Maintenance Scheduling Efficiency (97%). QKD technology, along with other quantum approaches, makes sure connected vehicle networks and smart transportation are strong against future quantum threats.

Future researchers may look into connecting QSPM with networks containing autonomous vehicles and electric vehicles, which will help reveal how well the system can be used on a larger scale. Studying multi-agent systems for decentralized maintenance and applying the model to multiple cloud systems would also be helpful, as they could improve QSPM's robustness.

If edge AI models are tweaked and used with different sensor data, they will give more precise forecasts in real-life scenarios. Even more, researchers could look into making blockchain updates so that the scheduling system can respond to external data whenever a car uses the resource.

References

[1] Dangeti Saivenkat Ajay, Sneegdh Krishnna, and Kavita Jhajharia, "Predictive Maintenance of NASA Turbofan Engines Using Traditional and Ensemble Machine Learning Techniques," *Advances in Distributed Computing and Machine Learning*, Singapore, vol. 660, pp. 369-379, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Stanley A. Melkumian, "Predictive Maintenance Analysis of Turbofan Engine Sensor Data," *The Journal of Purdue Undergraduate Research*, vol. 14, no. 8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] K. Sudharson, and Badi Alekhya, "A Comparative Analysis of Quantum-based Approaches for Scalable and Efficient Data Mining in Cloud Environments," *Quantum Information and Computation*, vol. 23, no. 9-10, pp. 783-813, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Usman Tariq et al., "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, pp. 1-46, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] K. Sudharson et al., "Quantum-Resistant Wireless Intrusion Detection System using Machine Learning Techniques," *2023 7th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, pp. 1-5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Dinesh kumar sah, Maryam Vahabi, and Hossein Fotouhi, "Federated Learning at the Edge in Industrial Internet of Things: A Review," *Sustainable Computing Informatics and Systems*, vol. 46, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Kumar Prateek et al., "A Privacy Preserving Authentication Protocol Using Quantum Computing for V2I Authentication in Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1-17, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Tannu Sharma et al., "Privacy Aware Post Quantum Secure Ant Colony Optimization Ad Hoc On-Demand Distance Vector Routing in Intent-Based Internet of Vehicles for 5G Smart Cities," *IEEE Access*, vol. 11, pp. 110391-110399, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Prashant Kumar et al., "Electric Vehicle Motor Fault Detection with Improved Recurrent 1D Convolutional Neural Network," *Mathematics*, vol. 12, no. 19, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Adva Hadrian et al., "DeepCAN: Hybrid Method for Road Type Classification Using Vehicle Sensor Data for Smart Autonomous Mobility," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 11, pp. 11756-11772, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jiaming Lai et al., "Blockchain-Based VANET Edge Computing-Assisted Cross-Vehicle Enterprise Authentication Scheme," *Computer Communications*, vol. 231, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mritunjay Shall Peelam et al., "Blockchain-Enabled Vehicle Lifecycle Management with Predictive Maintenance using Federated Learning," *IEEE Transactions on Consumer Electronics*, pp. 1-1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Nadeem Ahmed et al., "Advanced Machine Learning Approach for Dos Attack Resilience in Internet of Vehicles Security," *Heliyon*, vol. 10, no. 8, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Atul Barve, and Pushpinder Singh Patheja, "A Hybrid Deep Learning Based Enhanced and Reliable Approach for VANET Intrusion Detection System," *Cluster Computing*, vol. 27, no. 9, pp. 11839-11850, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Daniel S. Fowler, Carsten Maple, and Gregory Epiphaniou, "A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications," *Vehicles*, vol. 5, no. 4, pp. 1586-1604, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Alexandros Stavdas et al., "Quantum Key Distribution for V2i Communications with Software-Defined Networking," IET Quantum Communication, vol. 5, no. 1, pp. 38-45, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Salah Zidi et al., "Fault Prediction and Recovery Using Machine Learning Techniques and the HTM Algorithm in Vehicular Network Environment," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 5, pp. 132-145, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Hongyan Dui et al., "IoT-Enabled Fault Prediction and Maintenance for Smart Charging Piles," *IEEE Internet of Things Journal*, vol. 10, no. 23, pp. 21061-21075, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Zainab H. Ali et al., "SDN-based Reliable Emergency Message Routing Schema using Digital Twins for Adjusting Beacon Transmission in VANET," *Journal of Network and Computer Applications*, vol. 230, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Wenxian Jiang, Jun Tao, and Zhenglei Guan, "A Trusted Data Privacy Computing Method for Vehicular Ad Hoc Networks Based on Homomorphic Encryption and DAG Blockchain," *IEEE Internet of Things Journal*, vol. 12, no. 6, pp. 6621-6632, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Peng Hu et al., "An Efficient and Secure Data Collection Scheme for Predictive Maintenance of Vehicles," *Ad Hoc Networks*, vol. 146, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Syed Adnan Yusuf, Arshad Khan, and Riad Souissi, "Vehicle-To-Everything (V2x) in the Autonomous Vehicles Domain - A Technical Review of Communication, Sensor, and AI Technologies for Road User Safety," *Transportation Research Interdisciplinary Perspectives*, vol. 23, 2024. [CrossRef] [Google Scholar] [Publisher Link]