Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
 | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

Quantum-Safe Smart EV Charging and Secure Billing System Using IoT and Post-Quantum Cryptography

Chelsea Sharma[1], Dr. Abid Hussain[2]

[1]Student, Department of Computer Science, SRM Institute of Science and Technology, India

[2]Professor, School of Computer Application & Technology, Career Point University, Kota, Rajasthan, India

chelsea.sharma2311@gmail.com

Abstract: The rapid growth of electric vehicles (EVs) has created a strong demand for secure, intelligent, and reliable charging infrastructures. Most existing EV charging systems rely on classical cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are vulnerable to attacks from future quantum computers. This paper presents a quantum-safe smart EV charging and secure billing system implemented using low-cost Internet of Things (IoT) hardware and post-quantum cryptographic (PQC) algorithms.

The proposed system integrates RFID-based vehicle authenti- cation, real-time energy measurement, and secure offline billing. An ESP32 microcontroller controls the charging process through a relay module and collects voltage, current, and energy data from an energy meter sensor. Secure communication between the ESP32 and a Raspberry Pi server is achieved using CRYSTALS- Kyber for key exchange and CRYSTALS-Dilithium for digital signatures. The Raspberry Pi stores charging session logs and generates tamper-proof billing records based on actual energy consumption. The entire system operates offline on a local Wi-Fi network, ensuring privacy and reliability. Experimental results demonstrate the feasibility of deploying post-quantum cryptography on low-cost IoT hardware for future-ready EV charging systems.

Keywords: Electric Vehicles, IoT, RFID Authentication, Post-Quantum Cryptography, CRYSTALS-Kyber, Dilithium, Se- cure Billing, ESP32, Raspberry Pi

Introduction

Electric vehicles (EVs) play a vital role in reducing green- house gas emissions and dependence on fossil fuels. With the rapid increase in EV adoption, the need for secure and intelligent charging infrastructure has become critical. EV charging systems require secure communication between vehi- cles, charging stations, and backend servers for authentication,

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

billing, and control.

Most existing EV charging systems use classical crypto- graphic algorithms such as RSA, AES, and ECC. However, the emergence of quantum computing threatens these algorithms through quantum attacks such as Shor's algorithm. Long-term security is essential because EV charging infrastructure is expected to operate for many years.

Post-quantum cryptography (PQC) provides cryptographic algorithms that are resistant to both classical and quantum attacks. The National Institute of Standards and Technology (NIST) has standardized CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures. Integrating these algorithms into EV charging systems ensures future-proof security.

This paper proposes a practical hardware-based quantum- safe EV charging and secure billing system using low-cost IoT devices. The system provides RFID authentication, real-time energy measurement, offline operation, and tamper-proof billing.

Related Work

Several studies have focused on IoT-based EV charging sys- tems with cloud-based billing and scheduling. RFID technol- ogy has been widely used for user authentication in charging stations. These systems primarily use classical cryptographic techniques such as AES and RSA for secure data transmission. Recent research has proposed the integration of PQC into EV charging protocols such as ISO 15118. These works demonstrate the feasibility of PQC at the protocol level but remain limited to simulations and software models.

However, existing works do not address real-time energy measurement, hardware-based authentication, offline billing, and low-cost implementation. Most systems depend on cloud infrastructure, which limits their use in remote areas. This work bridges the gap by implementing a complete hardware prototype using IoT and PQC.

Problem Statement

Current EV charging systems suffer from the following limitations: Vulnerability to future quantum computing attacks. Dependence on cloud infrastructure for billing and au-thentication. Lack of real-time physical energy measurement. Absence of low-cost hardware-based secure prototypes. No provision for tamper-proof offline billing. Research Gap and

Motivation

The literature reveals the absence of a complete offline EV charging system secured with

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

post-quantum cryptography and validated through real hardware implementation. There is no integration of RFID-based physical authentication with PQC and real energy metering.

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

The motivation of this work is to bridge the gap between theoretical PQC-based protocols and real-world implementa- tion using affordable IoT hardware.

Proposed System Architecture

The proposed system consists of three layers:

Authentication Layer: Uses RFID reader to authenticate the EV via a unique RFID tag.

Control and Measurement Layer: ESP32 controls the relay module and measures voltage, current, and energy using the PZEM-004T energy meter.

Secure Billing Layer: Raspberry Pi acts as a local server for decrypting data, verifying signatures, and generating billing records.

The ESP32 and Raspberry Pi communicate securely using post-quantum cryptographic algorithms over local Wi-Fi.

Methodology

The working process is as follows:

RFID reader scans the EV tag and sends UID to ESP32.

ESP32 authenticates the EV and activates the relay.

Energy meter measures voltage, current, and energy.

ESP32 encrypts data using CRYSTALS-Kyber and signs using CRYSTALS-Dilithium.

Secure data is transmitted to Raspberry Pi.

Raspberry Pi decrypts and verifies data.

Billing is calculated as:

$$\text{Bill} = \text{Energy(kWh)} \times \text{Tariff} \quad (1)$$

Charging stops when EV is removed or threshold is reached.

Hardware Implementation

The hardware prototype includes:

ESP32 microcontroller

RC522 RFID reader

PZEM-004T energy meter

Relay module

Raspberry Pi

RFID card

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

Dummy load (LED bulb)

Security Framework Using PQC

The security framework uses:

CRYSTALS-Kyber for secure key exchange

CRYSTALS-Dilithium for digital signatures

This ensures confidentiality, integrity, and authenticity of charging data and protects against replay, man-in-the-middle, and quantum attacks.

Experimental Setup

A toy EV with an RFID tag and dummy load was used. Charging sessions were performed and energy readings were recorded. The Raspberry Pi generated billing records based on real-time energy usage.

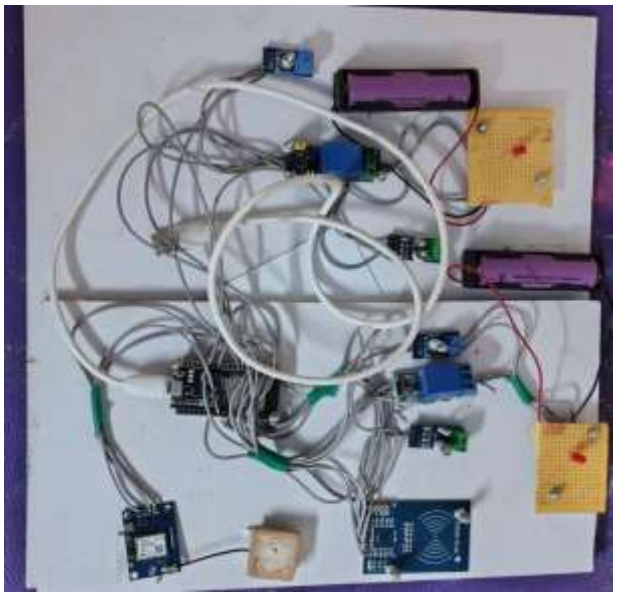

Figure 1 Overall Hardware Setup of the Proposed EV Charging System

Proceedings of International Conference on "Recent Innovations in Engineering, Technology & Science for Sustainable Development (RIETSSD-2026)"
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

Fig. 2. ESP32 microcontroller used for control and communication

Fig. 3. RC522 RFID reader and RFID card for vehicle authentication

Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

Fig. 4. Relay module and dummy load simulating EV battery

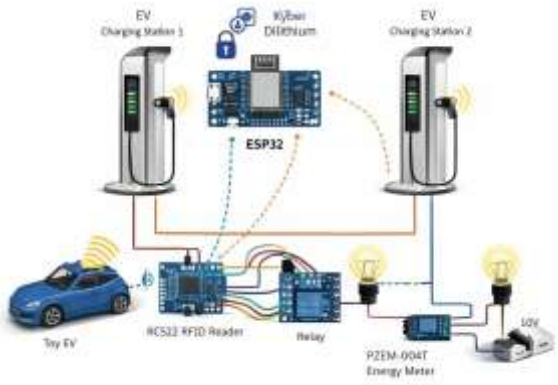

Fig. 5. System block diagram with PQC-based secure communication

Results and Discussion

The prototype successfully authenticated EVs, measured energy consumption, and generated secure billing records. PQC algorithms operated efficiently on low-cost hardware. The system functioned offline without cloud dependency.

Advantages and Limitations

Advantages:

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

Quantum-safe security

Offline operation

Low-cost hardware

Real-time billing

Tamper-proof records

Limitations:

Prototype-level system

Dummy load instead of real EV battery

Computational overhead of PQC algorithms

Conclusion

A quantum-safe smart EV charging and secure billing system using IoT and post-quantum cryptography has been presented. The hardware prototype validates the feasibility of PQC-based security for future EV charging infrastructure.

Future Work

Future work will include real EV integration, mobile appli- cation development, load management for multiple charging stations, and deployment in smart city environments.

References

[1] D. Kern, C. Krauß, T. Lauser, N. Alnahawi, A. Wiesmaier, and R. Niederhagen, "QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging," IACR Cryptology ePrint Archive, 2023.

[2] D. Kern et al., "QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging," in Applied Cryptography and Network Security (ACNS), Lecture Notes in Computer Science, Springer, 2023, pp. 85–111.

[3] A. B. Shahid, K. Mansoor, Y. A. Bangash, et al., "Post-quantum cryptographic authentication protocol for industrial IoT using lattice-based cryptography," Scientific Reports, 2026.

[4] R. Chowdhury, P. Dey, and S. Purkait, "Secure EV Charging and Communication: A Hybrid GNN-IDS and Post-Quantum Cryptographic Approach," in Proc. IEEE Int. Conf. Sustainable Energy and Future Electric Transportation (SeFeT), 2025.

CAREER POINT INTERNATIONAL JOURNAL OF RESEARCH
Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Special Issue | ISSN : 2583-1895
Conference Paper | DOI: https://doi.org/10.5281/zenodo.20470379

[5] Y. Liu, J. Ju, and Z. Li, "Privacy-Preserving Electric Vehicle Charging Recommendation Using Homomorphic Encryption and Secure Multi-Party Computing," World Electric Vehicle Journal, vol. 15, no. 10, 2024.

[6] T. M. Fernandez-Carames, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," arXiv preprint arXiv:2402.00790, 2024.

[7] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the Future Internet of Things with Post-Quantum Cryptography," arXiv preprint arXiv:2206.10473, 2022.

[8] T. Liu, G. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," arXiv preprint arXiv:2401.17538, 2024.

[9] K. Prateek, F. Altaf, R. Amin, and S. Maity, "A privacy-preserving authentication protocol for vehicular networks," Security and Communication Networks, 2022.

[10] A. Almadhor et al.,"Transfer learning for securing electric vehicle charging infrastructure from cyber-physical attacks," Scientific Reports, vol. 15, 2025.