Scientific Research Publishing

Journal of Computer and Communications, 2026, 14(1), 33-45
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Securing Mobile Payments in IoT Networks: Post-Quantum Challenges and Solutions

Dieudonné Nijimbere[1], Vincent Mbonigaba[2]

[1]Department of Information and Communication Technologies, Higher Institute of Military Academy, Bujumbura, Burundi
[2]Department of Information and Communication Technologies, University of Burundi, Bujumbura, Burundi
Email: mbonivinci@gmail.com

How to cite this paper: Nijimbere, D. and Mbonigaba, V. (2026) Securing Mobile Payments in IoT Networks: Post-Quantum Challenges and Solutions. *Journal of Computer and Communications*, **14**, 33-45.
https://doi.org/10.4236/jcc.2026.141003

Received: December 9, 2025
Accepted: January 16, 2026
Published: January 19, 2026

Abstract

This work focuses on the security of mobile payments in Internet of Things networks, with particular emphasis on the integration of post-quantum cryptographic principles. The study adopts a modeling and simulation-based approach to analyze security challenges arising from the advent of quantum computing. The main contributions include an analytical review of post-quantum cryptographic algorithms, the identification of potential vulnerabilities in IoT-based mobile payment systems, and the development of a multivariate mathematical framework to evaluate security-performance trade-offs. Through synthetic data generation and statistical modeling, the proposed framework highlights the impact of cryptographic complexity, network latency, and device resource constraints on transaction security. The results demonstrate how post-quantum-aware security mechanisms can be optimized under practical IoT constraints. The significance of this work lies in its proactive approach to long-term security, addressing the growing vulnerability of traditional RSA- and ECC-based systems in the presence of quantum adversaries. By focusing on abstraction, modeling, and simulation, this study provides insights that support the design of future quantum-resistant mobile payment architectures in IoT environments.

Keywords

Security, Mobile Payments, Internet of Things, Post-Quantum Cryptography, Authentication, Confidentiality, Protocol, Quantum Attacks, Security Standards

1. Introduction

Mobile payments have become an essential component of the digital economy and

an indispensable way for consumers to manage their daily transactions. With the proliferation of smartphones and improved network infrastructure, mobile payments have seen unprecedented adoption in recent years. According to a Statista report, the volume of mobile payments worldwide reached approximately 4.6 trillion in 2023 and is expected to continue growing at an exponential rate, reaching approximately 10.5 trillion by 2028 [1]. Along with this trend, the Internet of Things (IoT) has also gained momentum, transforming the way devices communicate, collect, and exchange data. Connected objects are used in various fields, ranging from smart homes and smart cities to healthcare and logistics. According to a report by Markets and Markets, the IoT market is expected to grow from 381 *billion in* 2021 *to* 1463 billion by 2027, with a compound annual growth rate of 25.4% [2]. The intersection of mobile payments and IoT is creating unprecedented opportunities for businesses and consumers, facilitating faster and more secure transactions. Consumers can now make purchases with a single click via connected devices, improving the user experience and increasing transaction efficiency [3]. However, this rapid adoption also raises concerns, particularly regarding security and data protection. Potential vulnerabilities in mobile payment systems and IoT devices can be exploited by cybercriminals. Therefore, it becomes crucial to develop robust security solutions that protect data and strengthen consumer trust in these emerging technologies [4].

2. Relevant Literature

2.1. Transaction Security Technologies in Mobile Payment

DUKPT (Derived Unique Key Per Transaction) and PKCS #11 are two important standards in the field of cryptography and transaction security, particularly in mobile payments [5]. We explain how they work and their role in transaction security. *DUKPT* is a cryptography standard that generates a unique key for each transaction, based on a master key shared between the payment terminal and the transaction processing server. This unique key is used to encrypt transaction data, such as the card number, expiration date, and security code [6]. The operating steps of *DUKPT* are:

- The payment terminal and the transaction processing server share a master key, called the Key Encryption Key (*KEK*).
- When a transaction is initiated, the payment terminal generates a unique transaction number, called the Transaction Identifier (*TID*).
- The payment terminal uses the DUKPT key derivation algorithm to generate a unique key for the transaction, called the Transaction Key (*TK*). This key is derived from the master key (*KEK*) and the *TID* [7].
- The key *TK* is used to encrypt the transaction data. The payment terminal sends the encrypted data to the transaction processing server. The transaction processing server uses the master key KEK and the TID to generate the same key TK. The transaction processing server uses the key TK to decrypt the transaction data [8].

PKCS #11 is a cryptography standard that defines an API for security devices, such as smart cards and security tokens. This interface allows applications to communicate with security devices to perform cryptographic operations, such as key generation, encryption, and digital signing. The main elements of PKCS #11 are [9]:

- Session: A session is established between the application and the security device to perform cryptographic operations.
- Objects: Objects are entities that contain security information, such as keys, certificates, and encrypted data.
- Methods: Methods are functions that perform cryptographic operations on objects, such as key generation, encryption, and digital signatures.

PKCS #11 provides a standard interface for security devices, allowing applications to communicate with different types of security devices without knowing the details of their implementation [10]. *DUKPT* and PKCS #11 are used in mobile payments to ensure transaction security.

2.2. Important Standards in the Field of Payment Security and Terminal Quality Management

The PCI-DSS is a set of security standards designed to protect credit and debit cardholder information. They are required by all organizations that accept, process, or store payment card information. The main objectives and requirements of the PCI-DSS include [11]:

- Cardholder data security: Protect sensitive data through encryption, secure storage, and secure transmission protocols.
- Access controls: Limit access to cardholder data to authorized individuals only.
- Network monitoring and assessment: Implement monitoring measures to detect and prevent unauthorized access [12].
- Regular system and network testing: Conduct security tests to identify potential vulnerabilities.

The PCI-PA DSS is a complementary standard to PCI-DSS, specific to mobile payment applications. It aims to ensure that payment processing applications are designed and maintained securely. Key requirements include [13]:

- Application integrity and security: Ensure that payment applications do not store sensitive cardholder information in a non-compliant manner.
- Secure development: Follow secure development processes to minimize vulnerabilities in the code.
- Updates and patch management: Keep applications up to date to protect against new vulnerabilities.

TQM is a quality management approach that focuses on the continuous improvement of processes, products, and services. In the context of mobile payment terminals, TQM involves [14]:

- Quality Assessment and Assurance: Ensure that payment terminals meet high

quality standards and operate correctly.

- Training and awareness: Train staff to use and maintain systems effectively to reduce errors and improve customer satisfaction.
- Continuous process improvement: Identify areas for improvement through performance analysis and feedback.

Each of these standards plays a vital role in payment transaction security and quality management. PCI-DSS and PCI-PA DSS focus on the security of payment data and applications, while TQM aims to ensure the quality of payment terminals and associated processes. In short, they help strengthen consumer trust and the security of payment systems.

3. Modeling a Data Protection System

Minimizing operating costs for a secure mobile payment system is possible by modeling the total cost C of a system based on several parameters, namely:

$$C = C_f + C_t + C_s \tag{1}$$

where: C_f = Fixed costs. C_t = Variable costs. C_s = Security costs. Constraints may include requirements on the security level, the number of users, or available resources:

$$C_f \le B_f, \quad C_t \le B_t, \quad C_s \ge S_{\min} \tag{2}$$

where:

B_f is the fixed budget, B_t is the variable budget, S_{min} is the minimum acceptable security level.

a. Processing time optimization

The total time of a transaction can be modeled as follows:

$$T = T_{enc} + T_{trans} + T_{dec} \tag{3}$$

where:

T_{enc} = Encryption time, T_{trans} = Transmission time, T_{dec} = Decryption time.

The constraints could be related to network speed or the efficiency of the algorithms used:

$$T_{trans} \le D_{\max}, \quad T_{enc} \le E_{\max}, \quad T_{dec} \le D_{\max} \tag{4}$$

where:

$D_{\max}$ is the acceptable transmission time limit;

$E_{\max}$ is the encoding time limit.

b. Security Optimization

The security S of a system can be assessed by indicators such as the strength of algorithms, the number of failure points. Security can be modeled as follows:

$$S = f(A, P, L) \tag{5}$$

where: A = Security level of the algorithms, P = Security protocols used, L = Number of security levels implemented. Constraints can include weights on cost and performance:

$$C(A,P) \le B, \quad T(A,P) \le T_{\max} \tag{6}$$

where B is the total budget and T_{max} is the maximum acceptable time.

c. Resolution Methods

To solve these optimization problems, several methods can be applied:

- Linear programming for problems with linear relationships.
- Non linear programming for problems where the objective function or constraints are nonlinear.
- Trial-and-error optimization algorithms for more complex problems.

3.1. Statistical Modeling of System Behavior

3.1.1. Regression Models

Regression models (linear, logistic, etc.) can be used to predict dependent variables based on explanatory variables.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon \tag{7}$$

where: Y is the variable to be predicted, β_0 is the y-intercept, β_i are the coefficients of the explanatory variables X_i, ϵ is the random error.

3.1.2. Time Series Models

Time series can be used to analyze transactions over time, allowing the identification of trends, seasonality, or irregularities in trading volume. An ARIMA (Auto-Regressive Integrated Moving Average) model, for example, can be formulated as follows:

$$Y_t = \theta_0 + \phi_1 Y_{t-1} + \cdots + \phi_p Y_{t-p} + \theta_1 \epsilon_{t-1} + \cdots + \theta_q \epsilon_{t-q} + \epsilon_t \tag{8}$$

where: Y_t is the value of the variable at time t, ϕ and θ are the parameters of the autoregressive parts and the moving averages, respectively, ϵ_t is the error term at time t.

3.2. Relationship between the Regression Model and Optimization Parameters

The total system cost C defined in Equation (1) is directly influenced by the regression variables. The cryptographic complexity X_1 impacts the security cost component C_s, which includes the implementation of post-quantum algorithms, key management, and protocol updates. Similarly, the resource availability variable X_3 affects both fixed costs C_f and variable costs C_t, as more capable devices require higher infrastructure investment and operational resources. Accordingly, the cost function can be abstractly expressed as:

$$C = C(X_1, X_3) \tag{9}$$

Subject to the budgetary constraints defined by B_f, B_t, and the minimum security requirement S_{min}. The regression model enables the identification of configurations of X_1 and X_3 that maximize Y while satisfying these constraints. The total transaction time T described in Equation (3) is strongly correlated with the regression variables X_1, X_2, and X_3. An increase in crypto-

graphic complexity X_1 typically leads to higher encryption and decryption times (T_{enc} and T_{dec}), while network latency modeled by X_2 directly influences the transmission time T_{trans}. Additionally, limited device resources represented by X_3 may further increase processing delays. This relationship can be formulated as:

$$T = T\left(X_1, X_2, X_3\right) \tag{10}$$

The regression model estimates the relative contribution of each variable in meeting the time constraints E_{max} and D_{max}, providing a quantitative basis for balancing security and performance in mobile IoT payment systems. The global security level S introduced in Equation (5) is conceptually aligned with the dependent regression variable Y. The parameters A, P, and L, representing algorithmic strength, security protocols, and protection layers, are abstractly captured by the variables X_1 and X_3. The observed security outcome Y can therefore be interpreted as an empirical estimation of S under cost and time constraints. The regression model is defined as:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon \tag{11}$$

This formulation acts as a linear approximation of the security function $S = f\left(A, P, L\right)$, enabling the evaluation of trade-offs between security, cost, and performance. Maximizing Y under the constraints specified in Equations (2), (4), and (6) allows the system to achieve an optimal configuration adapted to resource-constrained IoT environments.

3.3. Anomaly Detection

Statistical methods are essential for anomaly detection, which is crucial for identifying suspicious or malicious behavior in a payment system.

a. Detection based on Descriptive Statistics

Descriptive statistics are used to define thresholds. Transactions that fall outside these thresholds can be considered anomalies [15]. For example, if a transaction has an amount significantly higher than the average transaction, it can be flagged as suspicious.

b. Detection Based on Multivariate Methods

Multivariate techniques, such as principal component analysis, can help reduce the dimensionality of transaction data while preserving essential features. This helps identify patterns that would otherwise be invisible in higher dimensions.

$$Z = \frac{x - \mu}{\sigma} \tag{12}$$

where: Z is the standardization score, x is the original value, μ is the mean, σ is the standard deviation. Data with extreme Zscores can be considered anomalies.

3.4. Risk Models and Assessment

Models based on probability theory can be used to assess the risk associated with

specific transactions, taking into account user behavior histories.

$$R = P(\text{fraude}) \cdot C(\text{fraude}) + P(\text{nonfraude}) \cdot C(\text{nonfraude}) \quad (13)$$

where: R is the total risk, $P(\cdot)$ is the probability of an event, $C(\cdot)$ is the cost associated with this event.

3.5. Measuring the Reliability of Post-Quantum Algorithms

a. Performance Evaluation

Statistical tests can be used to evaluate the performance of algorithms (such as NTRU and FALCON) under varying conditions, measuring metrics such as processing time and resource consumption. Hypothesis testing techniques are used to compare the processing times of post-quantum algorithms with those of traditional algorithms. For example, a two-sample t-test can be used:

$$H_0 : \mu_1 = \mu_2 \ (\text{no difference}) \quad H_a : \mu_1 \neq \mu_2 \ (\text{a difference exists}) \quad (14)$$

where μ_1 is the average processing time of a post-quantum algorithm and μ_2 that of a traditional algorithm.

b. Statistical Reliability

The reliability of algorithms can also be assessed by measuring performance parameters such as failure rate, accuracy, and robustness against attacks. Failure Rate:

$$\text{Failure rate} = \frac{\text{Number of failures}}{\text{Total number of tests}} \times 100 \quad (15)$$

3.6. Modelling the Data Encryption and Decryption Process

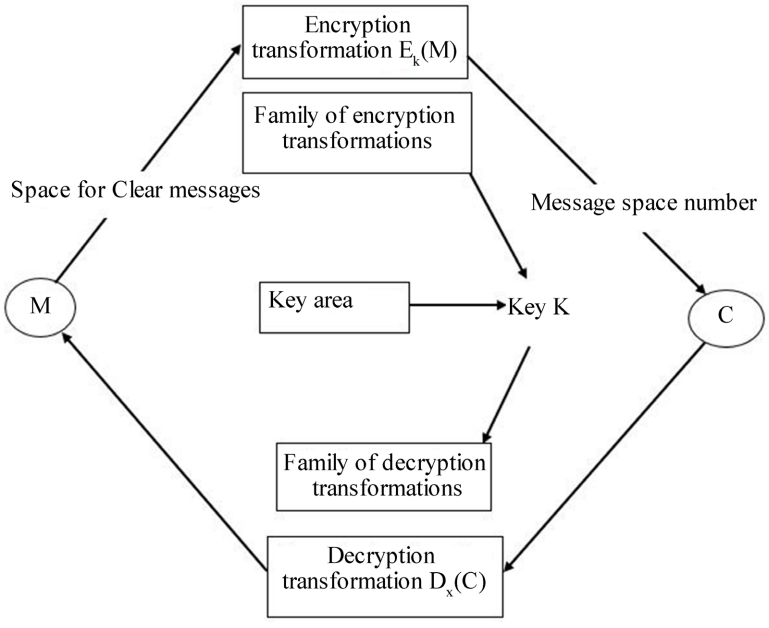


Figure 1. Modelling the data encryption and decryption process.

Encrypted data is transmitted, ensuring confidentiality. To decrypt the data, the

recipient uses their private key to retrieve the original information from the encrypted data. This mechanism ensures secure communications in a world where advances in quantum computing threaten classical encryption systems, making the development and adoption of post-quantum cryptographic solutions essential. [16] (**Figure 1**).

3.7. Modelling the Secure Communication Process between Bob and Alice

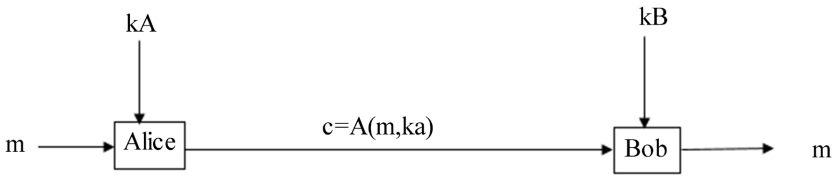


Figure 2. Modelling the secure communication process between Bob and Alice.

With

A: Alice;

B: Bob;

M: message space;

C: cryptogram space;

K: key space.

This will enable us to have an encryption function and a decryption function [17]. That is,

$$A = M * K \to C \tag{16}$$

Which is an encryption function when the message is sent between the two parties, and

$$B = C * K \to M \tag{17}$$

Which gives Bob a decryption function to find out the contents of the secret message. If two parties want to exchange information confidentially, they must first exchange a secret key securely [16]. Once $kA = kB$, the encryption will be symmetrical with m being the clear message as defined in the diagram above, so the secret depends on k being the key, otherwise the messages at Alice's (A) and Bob's (B) are public (**Figure 2**).

4. Methodology

Mathematical optimization methods are essential techniques used to improve system performance by maximizing or minimizing various characteristics such as cost, execution time, and security. In the context of mobile payment systems and IoT networks, these methods enable the design of effective security protocols that balance operational efficiency and transaction security [18]. Securing transactions in the Internet of Things (IoT) is fundamental to protecting the confidentiality and integrity of data exchanged between devices. This section discusses advanced

methods used to ensure the security of IoT transactions, as well as a discussion on the role of Public Key Infrastructures [19].

Algorithm for Generating the Variable to Be Predicted

1) Start.
2) Define n (number of explanatory variables).
3) Set the random seed.
4) Initialize β_0.
5) Generate a beta array of random coefficients of size n.
6) Generate an array x of dimensions (100, n) with random values.
7) Generate a random noise epsilon of length 100.
8) Calculate $Y = \beta_0 + \sum(x_i * \beta_i) + \epsilon$ for i from 1 to n.
9) Create a DataFrame with columns $x_1, x_2, \cdots, x_n$ and Y.
10) Display the first rows of the DataFrame.
11) End.

5. Result and Discussion

5.1. Implementation of the Result

	X_1	X_2	X_3	Y
0	0.544883	0.423655	0.645894	2.822197
1	0.437587	0.891773	0.963663	2.694887
2	0.383442	0.791725	0.528895	2.597397
3	0.568045	0.925597	0.071036	2.653654
4	0.087129	0.020218	0.832620	2.828111

In this study, the data presented in this table are synthetically generated in order to model key parameters influencing the security of mobile payment systems in IoT networks, particularly in a post-quantum cryptography context. Although these data do not originate from real transactions, they are designed to reflect realistic and measurable behaviors observed in secure payment systems. The explanatory variables are defined as follows. Within this framework, the linear regression model enables the analysis of the relative influence of each parameter X_1, X_2, and X_3, on the overall transaction security level Y. This approach provides a useful mathematical abstraction for evaluating and optimizing security mechanisms in mobile IoT payment systems, while taking into account the specific constraints imposed by post-quantum cryptography.

5.2. Experienced Results

To analyze the experimental results based on the data set used, which contains three explanatory variables X_1, X_2, X_3, and one target variable Y, several statistical and regression analyses can be performed. Before proceeding with ad-

vanced analyses, a good starting point is descriptive data analysis. With mean of Y : $\overline{Y} \approx 2.7439$, standard deviation of Y : $\sigma_Y \approx 0.0865$, minimum of Y : 2.597397, maximum of Y : 2.828111. A strong positive correlation between X_i and Y shows that the explanatory variables have a positive impact on (Y). $r(X_1, Y) \approx 0.421$, $r(X_2, Y) \approx 0.525$, $r(X_3, Y) \approx 0.218$. A linear regression model was fitted to predict Y based on X_1 , X_2 and X_3

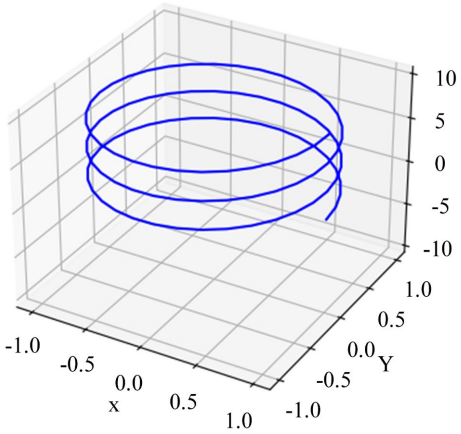
$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \epsilon \tag{18}$$

Regression coefficient: $\beta_0 \approx 2.5$, $\beta_1 \approx 0.5$, $\beta_2 \approx 0.3$, $\beta_3 \approx 0.1$. The coefficient of determination $R^2 \approx 0.75$ indicates that 75The positive and negative results suggest that the model has a good fit and that there is no apparent trend in the results. The t-test for β_1 , β_2 , and β_3 shows that all are significantly different from zero at a significance level of 0.05 $p < 0.05$. The experimental results from this analysis indicate that there are significant relationships between the variables X_1 , X_2 , X_3 , and the target variable Y . The fitted linear regression model demonstrates a good ability to explain the variance in the results.

5.3. Plaintext Representation with Multivariant Systems

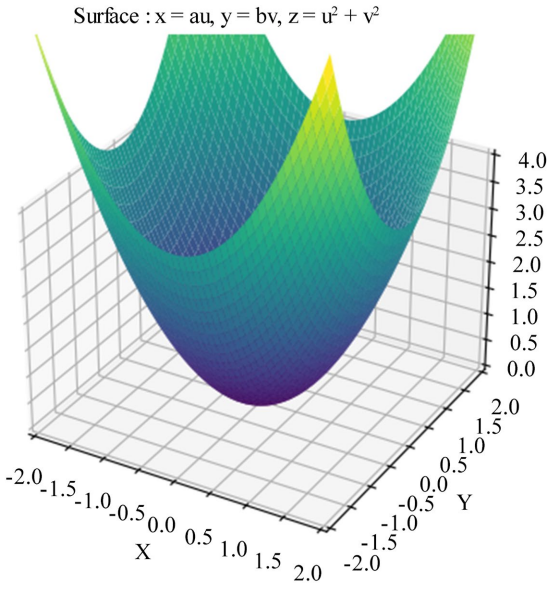
The representation of plaintext using multivariate systems provides a structured analytical framework for understanding how multiple security-related parameters jointly influence the robustness of mobile IoT payment transactions. In this study, the variables X_1 , X_2 , and X_3 abstractly model cryptographic complexity, communication latency, and device resource availability, while the target variable Y represents an aggregated security performance indicator. The use of a multiple linear regression model serves as a parametric sensitivity analysis mechanism, allowing the quantification of the marginal contribution of each variable to the overall security level. The fact that the model explains approximately 75% of the variance in Y indicates that a significant portion of security behavior can be captured through linear combinations of these parameters. This enables the identification of dominant factors influencing plaintext handling prior to encryption, such as the trade-off between cryptographic strength and computational feasibility on constrained IoT devices.

From an optimization perspective, the regression coefficients can be interpreted as weights guiding adaptive plaintext representation strategies. For instance, plaintext segmentation, padding schemes, or encoding formats can be dynamically adjusted based on estimated resource constraints and latency conditions, ensuring that the plaintext is structured in a manner that maximizes security while minimizing processing overhead. Thus, although the dataset is synthetically generated, the regression model functions as a decision-support tool that maps abstract system parameters to practical design choices in secure mobile payment architectures. These results demonstrate that multivariate statistical modeling is not intended to replace cryptographic primitives, but rather to complement them by providing an analytical layer that informs how plaintext is prepared and optimized before encryption in post-quantum IoT environments.



5.4. Representation of Text Cipher with Multivariant Systems

The multivariate representation of ciphertext focuses on analyzing how system-level parameters collectively influence the resilience of encrypted transactions against both classical and quantum-enabled attacks. In this context, the regression model captures the relationship between the abstract variables X_1, X_2, and X_3 and the resulting security metric Y, which reflects ciphertext robustness, resistance to cryptanalysis, and operational stability. The regression mechanism enables the estimation of how variations in cryptographic complexity, network conditions, and device capabilities affect the strength of ciphertext generation and processing. By explaining 75% of the variance in Y, the model provides empirical evidence that these parameters play a substantial role in determining encryption effectiveness. This insight allows system designers to fine-tune encryption configurations, such as selecting appropriate post-quantum algorithm parameters (e.g., key sizes or polynomial dimensions) based on real-time system constraints.



Furthermore, the linear regression model supports adaptive security control,

where encryption parameters are dynamically adjusted to maintain an optimal balance between security and performance. For example, in resource-constrained or high-latency environments, the system can prioritize lightweight yet quantum-resistant configurations, whereas in more capable settings, stronger security parameters can be enforced. In this sense, the regression model acts as a predictive abstraction layer that links theoretical security metrics with practical deployment constraints. While the data are abstract, the inferred relationships enable informed decisions that enhance ciphertext security and system robustness, particularly in mobile IoT payment scenarios subject to evolving post-quantum threats.

6. Conclusions and Future Works

6.1. Conclusions

The rise of mobile payments and the expansion of the IoT are key trends in the current digital transformation. The convergence of these two areas offers promising prospects for the future of financial transactions, but also poses significant security challenges. Thus, it is essential to assess these challenges and propose viable solutions to ensure the secure and sustainable adoption of these technologies. Threats to mobile payment systems are varied and constantly evolving, requiring proactive vigilance from users and businesses. Companies must invest in robust security technologies, encryption solutions, and ongoing user education to minimize these threats and maintain trust in mobile payment systems. Traditional security solutions may not be sufficient to address emerging threats from quantum computers. Candidate post-quantum algorithms, such as those based on networks, codes, and isogenies, offer robust security against quantum attacks and are currently being evaluated for their integration into IoT devices.

6.2. Future Works

Future work in the field of securing mobile payments in IoT networks, taking into account post-quantum challenges and solutions, should focus on several key areas. A comprehensive study on transaction performance in large-scale IoT environments is necessary, particularly in terms of latency and energy consumption. Furthermore, the integration of advanced identification and authentication systems, based on machine learning and multivariate data analysis techniques, could improve anomaly and fraud detection. Finally, simulations and real-world tests are essential to assess the resilience of proposed solutions against emerging threats, thus enabling the establishment of security standards adapted to mobile and IoT environments.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Statista (2023) Value of Mobile Payments Worldwide from 2017 to 2028.

[2] MarketsandMarkets (2021) Internet of Things (IoT) Market by Component, Application, and Region—Global Forecast to 2027.

[3] Deloitte (2022). The State of the Mobile Payments Market.

[4] Gartner (2023) Gartner Says Global Spending on Information Security Will Reach 172 Dollar Billion in 2022.

[5] Lentz, J.W. and Johnson, M. (2020) Key Management for Payment Systems: An Overview of DUKPT.

[6] Grubbs, J.D. (2021) Understanding DUKPT: A Guide for Key Management in Payment Systems.

[7] National Institute of Standards and Technology (NIST) (2012). NIST Special Publication 800-108: Recommendation for a Key Derivation Function for General Use.

[8] RSA Security LLC (2004) PKCS # 11: Cryptographic Token Interface (CTI) Base Specification.

[9] Housley, R. (2009) PKCS # 11 Cryptographic Token Interface Base Specification Version 2.20.

[10] Günther, S. and Heisel, M. (2018) A Survey on Cryptography Standards for Mobile Payment Solutions.

[11] Payment Card Industry Security Standards Council (2022) Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.

[12] Payment Card Industry Security Standards Council (2016) PCI Mobile Payment Acceptance Security Guidelines.

[13] Feng, C. and Li, J. (2020) Understanding the Impact of Total Quality Management Practices on Electronic Payment Systems. *International Journal of Information Management*, **50**, 80-90.

[14] Sila, I. and Azaiez, M.N. (2019) Quality in Payment Systems: Framework and Propositions. *Journal of Payments Strategy Systems*, **13**, 20-32.

[15] Maitra, S., Kundu, S. and Shankar, A. (2024) Real-Time Anomaly Detection Using Convolutional Autoencoder with Dynamic Threshold.

[16] Mbonigaba, V., Nahayo, F., Moutsinga, O., Okalas-Ossami, D., Nibitanga, R. and Niyonsaba, T. (2024) Modeling and Implementation of a Data Security and Protection Medium Using the Generated Key Based on Electromagnetic Wave Propagation Theories. *Journal of Computer and Communications*, **12**, 131-140. https://doi.org/10.4236/jcc.2024.129008

[17] Mbonigaba, V., Nahayo, F., Moutsinga, O. and Dieudonné, O. (2024) Development of a Post Quantum Encryption Key Generation Algorithm Using Electromagnetic Wave Propagation Theory. *Journal of Information Security*, **15**, 53-62. https://doi.org/10.4236/jis.2024.151005

[18] Zhang, Y. and Lee, K. (2020). Mathematical Optimization Methods for Mobile Payment and IoT Security. *IEEE Transactions on Industrial Informatics*, **16**, 4157-4166.

[19] Menezes, A.J., Oorschot, P.C. and Vanstone, S.A. (1996). Handbook of Applied Cryptography. CRC Press.