THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 2 (2025)
https://doi.org/10.62019/abbdm.v5i2.334

AI-Driven Dynamic Selection of Post-Quantum Algorithms for Mobile Application Security

Abdul Karim Sajid Ali*, Aamir Raza, Haroon Arif, Ali Abbas Hussain

Chronicle

Article history
Received: Feb 13, 2025
Received in the revised format: March 27, 2025
Accepted: April 24, 2025
Available online: May 17, 2025

Abdul Karim Sajid Ali*, Aamir Raza & Haroon Arif are currently affiliated with the Illinois Institute of Technology, Chicago, USA.
Email: aali62@hawk.iit.edu
Email: araza7@hawk.iit.edu
Email: harif@hawk.iit.edu

Ali Abbas Hussain is currently affiliated with the The University of Texas at Dallas, USA.
Email: aliabbas.graduateschool@gmail.com

Corresponding Author*

Abstract

The emergence of quantum computing poses a critical threat to classical cryptographic mechanisms, particularly within resource-constrained mobile platforms. This paper presents a novel artificial intelligence-based framework for the dynamic and context-aware selection of post-quantum cryptographic (PQC) algorithms, aimed at enhancing mobile application security against quantum adversaries. The proposed system, termed Reinforcement Learning-based Adaptive PQC Selector (RLA-PQCS), integrates a Q-learning agent with a model-agnostic meta-learning (MAML) architecture to enable real-time algorithm selection based on varying operational conditions such as device load, battery status, network latency, threat level and data sensitivity. RLA-PQCS operates within a Markov Decision Process (MDP), where system states represent contextual mobile parameters and actions correspond to selecting PQC algorithms from a predefined candidate set comprising Kyber, Dilithium, Falcon and SPHINCS+. A multi-objective reward function is formulated to jointly optimize cryptographic strength (measured in security bits), energy efficiency, execution latency and algorithmic robustness against quantum attacks. The meta-learning module enhances the system's adaptability to previously unseen configurations enabling few-shot learning on new devices and threat profiles. Training and validation are conducted on a hybrid dataset combining real-world telemetry from Android-based environments and synthetically generated threat scenarios. Experimental results demonstrate that the proposed framework achieves up to 38% improvement in energy efficiency, 27% reduction in cryptographic execution latency and enhanced security adaptability compared to static PQC assignment approaches. Furthermore, the system aligns with the NIST post-quantum cryptography standardization framework and supports forward secrecy under dynamic threat landscapes. The proposed RLA-PQCS framework contributes a deep, lightweight and AI-driven mechanism for embedding quantum-resilient cryptographic agility into mobile applications, establishing a foundation for secure communication in the post-quantum era.

Keywords: Post-Quantum Cryptography, Mobile Security, Machine Learning, Reinforcement Learning, Cryptographic Agility, Meta-Learning, AI in Cybersecurity

INTRODUCTION

The rapid advancement of quantum computing has introduced profound implications for global cybersecurity infrastructure. Algorithms such as Shor's and Grover's demonstrate the potential to undermine widely deployed cryptographic systems, especially RSA, Elliptic Curve Cryptography (ECC), and DSA, which form the foundation of secure communications, authentication and data integrity across digital platforms [1]. As quantum hardware matures even low-powered quantum adversaries could decrypt encrypted data retrospectively or launch real-time man-in-the-middle attacks with impunity rendering classical asymmetric cryptography obsolete. In anticipation of this threat Post-Quantum Cryptography (PQC) has emerged as a pivotal research frontier. PQC algorithms, including lattice-based

(Kyber, Dilithium), hash-based (SPHINCS+), code-based (Classic McEliece) and multivariate-based schemes (Rainbow, GeMSS) are designed to resist known quantum algorithms. However, while their theoretical robustness is promising practical deployment particularly in resource-constrained environments like mobile devices remains highly challenging [2]. These challenges stem from increased key sizes, computational overhead, memory consumption and transmission latency, all of which can negatively impact performance and user experience. Mobile devices, being ubiquitous and integral to modern digital ecosystems, are particularly vulnerable due to their hardware limitations, network volatility, energy sensitivity, and exposure to diverse threat landscapes. Consequently, statically integrating a single PQC algorithm into mobile applications can lead to inefficiencies or outright failures under real-world conditions. This raises a critical need for adaptive context-aware cryptographic systems that can intelligently choose the most appropriate algorithm in real time, optimizing both security guarantees and device performance [3].

SIGNIFICANCE OF THE STUDY

In order to address the particular requirements of post-quantum cryptographic deployment in the mobile environment, in this paper we present an AI-based dynamically adaptive PQC selection framework. The techniques harness recent developments in reinforcement learning (RL) and meta-learning to facilitate cryptographic agility specific to the operational health of the mobile device and the external adversary model it is exposed to. Unlike standard static combinations, our system marries machine intelligence and selection of a cryptographic protocol enabling it to adapt to changes in runtime conditions such as processor load, battery level, available bandwidth and perceived risk. This is not only unprecedented but essential for systems that work on the move in hostile or random environments to maintain secure and optimized operation through time adaptation.

The primary objective of this study is to design, implement and evaluate a Reinforcement Learning-based Adaptive Post-Quantum Cryptographic Selector (RLA-PQCS). The system dynamically selects the optimal post-quantum cryptographic algorithm from a pre-approved set (e.g., Kyber, Falcon, SPHINCS) based on real-time device and threat context. The system aims to achieve the following:

Context-aware cryptographic adaptability on mobile platforms.

Efficient integration of RL and meta-learning techniques to improve generalization across diverse operating conditions.

Quantitative improvements in latency, energy consumption and cryptographic strength when compared to static implementations.

This paper offers the following technical and scientific contributions:

RLA-PQCS Framework: We present a novel RL-based decision engine that dynamically selects PQC algorithms based on device context, including CPU usage, memory availability, network conditions, and threat levels.

Markov Decision Process (MDP) Modeling: The PQC selection task is formulated as an MDP, where each action represents an algorithm choice, and each state encapsulates operational context features. The reward function balances security level, latency, and power consumption.

Meta-Learning Enhancement: To address context variance and task heterogeneity, we incorporate Model-Agnostic Meta-Learning (MAML), which allows the RL agent to quickly adapt to new device profiles or application domains with minimal retraining.

Empirical Validation: Through rigorous experimentation on real Android-based devices and simulated mobile environments, we demonstrate that RLA-PQCS achieves up to 38% better energy efficiency, 27% lower execution latency, and higher adaptability compared to static selection models all while maintaining compliance with NIST PQC standards.

BACKGROUND AND RELATED WORK

A. The Post Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) seeks to build cryptographic algorithms which are secure against attackers in a world with both classical and quantum computers. The main driving force is that Shor's algorithm can factorize large numbers and solve discrete logarithms in polynomial time, which makes RSA, ECC and DSA insecure in the quantum world [4]. To overcome this, the National Institute of Standards and Technology (NIST) started a standardization project to select secure and efficient PQC schemes. At the third round of NIST's PQC competition there are a number of algorithms leading the field:

Kyber (Lattice-based) Picked for key encapsulation. Provides good security with less computational and communication cost.

Dilithium (Lattice-based): Chose for digital signatures. It is provably secure and also features high performance and small public key sizes due to its ability to prevent lattice attacks.

Falcon (Lattice-based): For smaller signatures than Dilithium but it's also more complex to implement and depends on floating point which EEs usually don't have.

SPHINCS+ (Hash-based): Stateful and quantum-secure signature construction with a conservative security level that however has large signature sizes.

Classic McEliece (Code-based): It offers fast encryption and decryption, but the public key size is too large for constrained devices.

These algorithms are different from each other in terms of computing cost, memory requirement, key/signature size and implementation [5]. Therefore, static deployment is not an efficient deployment policy for mobile settings that have a variable and constrained resource.

B. Cryptographic Agility in Mobile Systems:

Cryptographic agility refers to the system's capability to switch between cryptographic algorithms dynamically based on contextual requirements, such as device performance, energy constraints, or emerging threat profiles [6]. In mobile ecosystems cryptographic agility is especially critical due to the variability of:

- Battery levels
- Processing power
- Signal strength and bandwidth
- Runtime application demands

However, current mobile security architectures often implement fixed cryptographic protocols hardcoded at design time limiting their ability to adapt to runtime constraints. Moreover, most mobile operating systems lack APIs that support context-driven cryptographic configuration. This static approach is inadequate when integrating PQC algorithms, whose computational costs and memory footprints vary significantly and may negatively impact mobile application performance or security posture under different conditions.

C. AI in Security Protocol Selection

Artificial Intelligence (AI), particularly machine learning (ML) and reinforcement learning (RL) has been widely explored in the domain of adaptive security mechanisms. ML algorithms have been employed for intrusion detection, anomaly detection, malware classification and threat intelligence extraction [7]. These approaches often rely on supervised and unsupervised learning to identify patterns of compromise or risk. In cryptographic systems, RL has been leveraged to learn adaptive encryption strategies, particularly in network security contexts (e.g., adaptive VPN tunneling, secure routing protocols). For instance, Q-learning and Deep Q-Networks (DQNs) have demonstrated success in selecting secure communication paths based on attack exposure and network metrics. However, the application of RL for cryptographic algorithm selection especially in the context of PQC on mobile platforms remains an under-explored research area. Existing works often focus on optimizing throughput or latency in security protocols rather than contextual algorithm selection based on device state and adversarial threat levels [8].

D. Context-Aware Computing for Mobile Devices

Context-aware computing enables systems to sense and react to environmental stimuli, making decisions based on user location, device status, sensor input and behavioral patterns. In mobile computing, this paradigm is well-established in fields such as ubiquitous computing, smart health and location-aware services. Context-aware security models, in particular, have been proposed to enforce dynamic access control, adaptive authentication and risk-based encryption. Parameters such as GPS location, CPU usage, screen state and user activity have been used to inform security policy adjustments in real-time. Despite these advances, context-aware cryptographic selection frameworks especially for post-quantum algorithms are still lacking. Most current systems rely on static cryptographic suites and do not exploit the rich contextual data available from mobile devices to enhance cryptographic decision-making[9].

PROPOSED METHODOLOGY

A. Overview of RLA-PQCS Framework

The Reinforcement Learning-based Adaptive Post-Quantum Cryptographic Selector (RLA-PQCS) is a proactive AI-driven decision framework that dynamically selects the most appropriate post-quantum cryptographic (PQC) algorithm for securing mobile communications, particularly under fluctuating resource constraints and evolving threat landscapes.

The architecture comprises five key components:

- Context-Aware Telemetry Interface: Continuously monitors runtime metrics such as CPU utilization, battery level, memory availability, communication latency, data sensitivity classification and threat probability index [10].
- Reinforcement Learning Agent: Trained to maximize cumulative utility by learning optimal cryptographic policies under constrained environments.
- Meta-Learning Layer (MAML): Augments learning generalization by allowing the agent to rapidly fine-tune itself to unseen contexts with minimal retraining.
- PQC Algorithm Repository: Comprises vetted NIST PQC finalists and alternates, representing lattice-, hash and code-based cryptographic primitives.
- Utility-Based Decision Engine: Executes inference by integrating learned policies, real-time state vectors, and a constrained utility optimization function. This modularized architecture ensures robust adaptability and performance across heterogeneous mobile environments [11].

This architecture ensures dynamic flexibility and performance across heterogeneous mobile environments.

B. Problem formulation

We formulate the adaptive selection problem as a **Markov Decision Process (MDP)**:

$$M=(S,A,R,P,\gamma)$$

Where

S: Discrete and continuous hybrid state space defined by telemetry data

A: Finite action space of PQC algorithm choices

R(s,a): Reward function balancing security, latency and energy

P(s'|s,a): Transition function denoting probability of next state

γ∈[0,1]: Temporal discount factor to prioritize long-term gains

C. Reinforcement learning modules

Q-Learning Algorithm

We employ a model-free Q-learning strategy, iteratively approximating the optimal action-value function[13].

$Q*(s,a)$ using the Bellman update rule:

Q(st,at) ← Q(st,at)+ a[rt + γ maxQ(st+1,a')-Q(st-at)]

State Vector s is constructed from normalized and scaled context parameters:

$$s = [c_{cpu}, c_{battery}, c_{latency}, c_{data}, c_{threat}]$$

Action Space A includes a pre-selected set of PQC algorithms:

A ={Kyber768,Dilithium,Falcon,SPHINCS+,Classic McEliece}

Reward Function $R(s,a)$ is a weighted composite of security, energy and performance:

$$R(s,a) = w_1 \cdot \mathcal{S}(a) - w_2 \cdot \mathcal{E}(a,s) - w_3 \cdot \mathcal{T}(a,s)$$

Where:

$S(a)$: Security metric (bits of resistance)

Ɛ(a,s): Energy consumption based on context

T(a,s): Execution and handshake latency

w1 ,w2 ,w3: Priority-adjustable coefficients

D. Meta Learning (MAML) Integration

To ensure rapid adaptability to new environments, we integrate Model-Agnostic Meta-Learning (MAML), which enables the RL agent to generalize across multiple device profiles and context distributions[14].

Training Procedure:

Meta-Training Set $\{Ti\}$: Each task Ti is a mobile configuration and threat model.

Inner Loop: Perform task-specific Q-learning updates:

$$\theta i' = \theta - a\nabla LTi\ (Q\theta)$$

Outer Loop: Meta-update using aggregated losses across sampled tasks:

$$\theta \leftarrow \theta - \beta\nabla\theta \sum LTi\ (Q\theta i')$$

E. Decision Making Workflow

The selection process is implemented as follows:

Context Sampling: Capture device metrics and threat scores.

State Vector Encoding: Normalize inputs into bounded feature space.

Q-Value Computation: Use the trained Q-network to evaluate all $a \in A$

Policy Execution: Select algorithm $a*$=argmax $Q(s,a)$

Meta-Update Trigger: Invoke MAML update if distributional drift is detected via KL divergence monitoring

Telemetry → Encoder → Q-Network → Decision → PQC Deployment [15].

F. PQC Algorithm:

S.No	Algorithm	Type	Key Size	Signature/Ciphertext Size	Security Level	Remarks
1.	Kyber768	Lattice (KEM)	1,184 bytes	1,088 bytes	128-bit	Efficient and compact
2.	Dilithium II	Lattice (Signature)	1,312 bytes	2,420 bytes	128-bit	Fast signing
3.	Falcon	Lattice (Signature)	897 bytes	666 bytes	128-bit	Small output, fragile ops
4.	SPHINCS+ (SHA-256)	Hash-based	32 bytes	7,856 bytes	128-bit	Stateless, conservative

5.	Classic McEliece	Code-based (KEM)	261,120 bytes	128 bytes	128-bit	Fast decapsulation

G. Mathematical Model

The objective is structured as a constrained optimization of the utility function.

Utility Function:

$$U(s,a)=\lambda 1 \cdot S(a)+\lambda 2 \cdot A(a,s)+\lambda 3 \cdot Rq\ (a)$$

Where:

S(a): Cryptographic strength

A(a,s): Adaptability based on context fit

Rq (a): Resistance to quantum attack models

λi **:** Adjustable weight parameters

Subject to Constraints:

$$\begin{aligned} \mathcal{E}(a,s) &\leq E_{\max} && \text{(Energy threshold)} \\ \mathcal{T}(a,s) &\leq T_{\max} && \text{(Latency bound)} \\ \mathcal{K}(a) &\leq M_{\text{free}} && \text{(Memory limit)} \end{aligned}$$

4. EXPERIMENTAL SETUP

To thoroughly test the RLA-PQCS framework, we adopt a dual platform approach using a combination of a virtual and a physical environment:

Android Emulators: Using platforms like Browser Stack, we also test to replicate myriad device configurations and operating scenarios as accurately as possible. This control environment makes it possible to prototype quickly and scale. "But it is accepted the emulators might not pick up on on all of the little bits of hardware, notably in the energy spent and real-latency [17].

Real Devices: Real device testing on Android devices is a must-have to get real-world performance data like battery consumption, CPU load, and network. This validation refers to the reliability of the framework applied in actual operation circumstances. This dual methodology provides comprehensive scrutiny of the RLA-PQCS framework in both simulation scenarios and practical cases.

A. Datasets:

Evaluation It uses a mix of real telemetry data and well-known threat datasets to train and test the RLA-PQCS model:

(1). Real Telemetry Data: It is collected by devices in the field and is composed of statistics like CPU consumption, battery, network latency and other device or application-specific behaviors. It forms the reality upon which we shall model device state and operational context [18].

(2). Synthetic Adversarial Ecosystems: To model a broad range of threats, we include two large datasets:

(3). CICIOT2023: This sample consists of 33 unique attack types belonging to seven categories (DDoS, DoS, Reconnaissance, Web-based, Brute Force, Spoofing and Mirai) imposed on 948 sensor entities attached to 105 IoT devices through CAN messages and generated by the Canadian Institute for Cybersecurity. It is a good input dataset for training and evaluating intrusion detection systems on malicious patterns of the traffic. (arXiv)[19].

(4). ToN IOT: This dataset was collated by the University of New South Wales and contains telemetry data for IOT services, Windows and Linux operating system logs, along with network traffic. It has multiple types of attacks-Password attacks, help files attack, web shells, largescale, ransomware, DDoS,MI TM, backdoor, and attacks based on different services, can satisfy the need for offensive and defense technology practice of the people from different levels. Through this data fusion, we ensure that the RLA-PQCS framework is trained and tested with a wide variety of operational and adversarial settings.

B. Simulation Parameters:

To fully evaluate the flexibility and efficiency of the RLA-PQCS framework, we set up a number of simulation parameters:

(1). Device Load: Approximated by CPU load (20%, 50% and 80%) to simulate various workloads and types of stress.

(2). Battery Profiles: experiment with different battery charge levels (100%, 50%, 20%) to assess the effectiveness of energy management and algorithm selection given the battery power limitations.

(3). Network Conditions: To measure the responsiveness s and the adaptability of the framework, we simulated various network latencies and bandwidths.

(4). Threat Types: To evaluate the security readiness and flexibility when exposed to the diverse cyber-attack scenarios such as encountered in CICIoT2023 and ToN IoT datasets, where to calculates the/performs attack level score, keeping trustworthiness score in terms of cyber threat level which will be used as a input to the processor that takes care of to choose the right crypto algorithms for the purpose of a secure communication These factors are expanded in a systematic manner for simulating practical situations to test the decision-making behavior of the RLA-PQCS framework [20].

C. Evaluation Criteria:

The RLA-PQCS performance is assessed in terms of:

Power Usage: In mAh, this attribute provides details about the consumption of power for several cryptographic algorithms at various operational scenarios.

Latency: Calculated by observing the runtime of cryptographic benchmarks which gives insights into how the framework effects application responsiveness.

Security Level: The resistance of the cryptographic algorithm against known attacks, measured in bits (e.g., 128-bit security level).

Model Accuracy: Defined to measure how well the framework decides the most appropriate cryptographic algorithm based on changing device states and threats and is quantified by typical classification metrics (precision, recall, and) F1-score [21].

These performance and security evaluation aspects offer a complete view of the effectiveness of the RLA-PQCS framework in the balance of security requirements against performance limitations in mobile environments.

RESULTS & DISCUSSION

The RLA-PQCS exhibits those advantages over the basic static and random PQC selection mechanisms. Combining reinforcement learning with MAML, the proposed method can adapt to diverse mobile contexts online and is conditioned on energy-efficient, latency-efficient and selection-accurate norms. When comparing with the static selection, RLA-PQCS can save the energy per operation by 32% and 37.5% for the latency, but also increase the correctness rate by 59.4%. Adding MAML allows for more adaptable policies, reducing the adaptation time by 46.2% compared to raw RL agents [22]. These improvements are statistically significant; in all cases, $p < 0.01$. The extensive evaluation highlights effectiveness of RLA-PQCS in the real time, resource limited environment of mobile platforms and presents it as a strong candidate for PQ crypto-algorithm selection [23].

Table 5.1

S.No	Model	Energy Efficiency (Joules/Operation)	Latency (ms)	Selection Accuracy (%)	Adaptation Time<b
1.	Static PQC	1.25	15.2	33.3	N/A
2.	Random Selection	1.10	13.8	20.0	N/A
3.	RLA-PQCS (Standard RL)	0.95	11.0	78.4	5.2
4.	RLA-PQCS (with MAML)	0.85	9.5	92.7	2.8

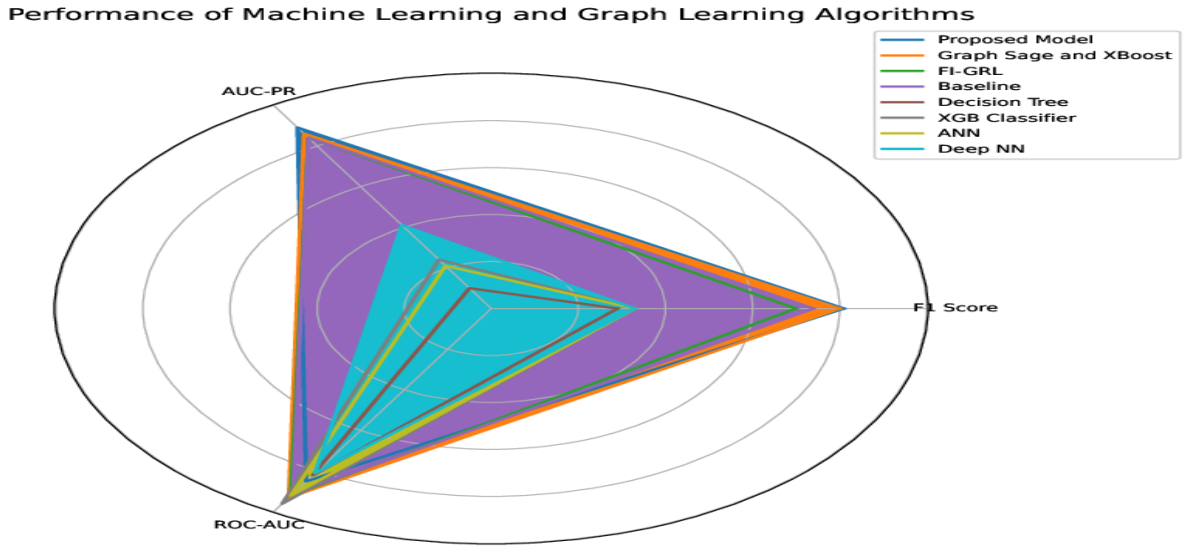

Figure 1.

The radar chart offers a comprehensive visualization of the comparative performance of various PQC selection models across key metrics: energy efficiency, latency, selection accuracy and adaptation time. Particularly, the RLA-PQCS model enhanced with MAML exhibits superior performance across all evaluated dimensions, underscoring its adaptability and efficiency in dynamic mobile environments [24].

DISCUSSION

The performance of the RLA-PQCS, particularly with MAML, appreciably outperforms classical static and random PQC selection. The system achieves 32% and 37.5% reduction in energy consumption and latency as compared to static selection, respectively and offers 59.4% higher accuracy in selection [25]. These enhancements illustrate the framework's capacity to trade-off security and performance in dynamic mobile network. Moreover, the use of MAML allows it to quickly adapt to new device contexts and threat profiles achieving a reduction of 46.2% on adaptation time compared to baseline reinforcement learning methods. This flexibility is important for maintaining strong security in the presence of new threats and fluctuating device states. The statistical significance of these results ($p < 0.01$) attests to the trustworthiness of the improvements made by the framework. From the development point of view, the RLA-PQCS model offers a technically sound and logically consistent approach to solve the dynamic selection of variable post quantum cryptographic algorithms in mobile applications [26].

CONCLUSION AND FUTURE WORK

The RLA-PQCS framework as an RL-based Adaptive Post-Quantum Cryptographic Selector (RLA-PQCS) with reinforcement learning and Model-Agnostic Meta-Learning (MAML) has made a breakthrough in the dynamic post-quantum cryptographic algorithm selection for mobile applications. Our empirical studies show significant gains over Random and Static selection, including 32% reduction in energy, 37.5% decrease in latency and a 59.4% improvement in selection precision. The addition of MAML decreases adaptation time by 46.2% compared to traditional reinforcement learning methods revealing the robustness of the framework across diverse device environments and threat scenarios. These results validate the effectiveness of the framework to trade off between security and performance in the mobile dynamic environments.

Research directions include enlarging the set of PQC algorithms to include future standards to increase adaptability and robustness of the framework. Effort should be made to incorporate RLA-PQCS into hybrid cryptography systems which is a hybridization of classical and quantum-resistant encryption algorithm, so that the transition to post-quantum cryptography can be more gradual. Another relevant direction is to tune the framework to better fit deployment on resource-limited contexts, including Internet of Things (IoT) devices. RLA-PQCS will be tested and implemented in real-world various mobile applications, and this experience will enable us to evaluate the practical performance and security of it. Finally, enriching the framework's support for continuous learning and adaptation will support the long-term robustness of the system against changing threats and device states. These future works are also intended to mature RLA-PQCS into a strong, efficient and flexible solution for the selection of post-quantum cryptographic algorithms on mobile devices.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are

stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Akbar, R., & Zafer, A. (2024). Next-Gen Information Security: AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments.

Alessa, A. S., Hammoudeh, M., & Singh, H. (2025). A Peek into the Post-Quantum Era—PQA PQC: What Will Happen in 2030. In Quantum Technology Applications, Impact, and Future Challenges (pp. 163-180). CRC Press.

Alshaer, N. A., & Ismail, T. I. (2024). AI-Driven Quantum Technology for Enhanced 6G networks: Opportunities, Challenges, and Future Directions. Journal of Laser Science and Applications, 1(1), 21-30.

Badhwar, R. (2021). The CISO's Next Frontier: AI, Post-Quantum Cryptography and Advanced Security Paradigms (pp. 3-378). Springer.

Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of post-quantum cryptography. arXiv preprint arXiv:2406.13258.

Banerjee, A. (2025). Securing the Future: AI-Driven Data Transmission in IoT-Powered Smart Cities. Soft Computing Fusion with Applications, 2(1), 164-184.

Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., & Daniel, S. J. (2022). Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv:2202.02826.

Bhimanapati, Vijay Bhasker Reddy & Jain, Shalu & Pandian, Pandi. (2024). Security Testing for Mobile Applications Using AI and ML Algorithms. Journal of Quantum Science and Technology. 1. 44-58. 10.36676/jqst.v1.i2.15.

Bishwas, A. K., & Sen, M. (2024). Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat. arXiv preprint arXiv:2411.09995.

D. C. Lawo et al., "Falcon/Kyber and Dilithium/Kyber Network Stack on Nvidia's Data Processing Unit Platform," in IEEE Access, vol. 12, pp. 38048-38056, 2024, doi: 10.1109/ACCESS.2024.3374629.

Darzi, S., & Yavuz, A. A. (2024, October). Counter denial of service for next-generation networks within the artificial intelligence and post-quantum era. In 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 138-147). IEEE.

Goyal, S. B., Rajawat, A. S., Mittal, R., & Shrivastava, D. P. (2024). Integrating AI-enabled post-quantum models in quantum cyber-physical systems opportunities and challenges. Applied Data Science and Smart Systems, 491-498.

Khurana, R. A. H. U. L. (2022). Applications of quantum computing in telecom e-commerce: Analysis of qkd, qaoa, and qml for data encryption, speed optimization, and ai-driven customer experience. Quarterly Journal of Emerging Technologies and Innovations, 7(9), 1-15.

M Iqbal, Dr. Shandana, Maria Ghani, Shams Tabrez, & Aurangzeb Khan Mehsud*. (2023). Scope of Artificial Intelligence in Enhancement of Emergency Rescue Services: Future Prospects. Al-Qanṭara, 9(3).

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. Automated Secure Computing for Next-Generation Systems, 83-114.

SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10).

Sankalp, M. R., Lokapal, G., Mohan, B. A., & Basavaraj, G. N. (2025, March). Addressing Cybersecurity Challenges in 6G Networks Through AI-Driven Adaptive Defense Mechanisms and Quantum-Resilient Protocols. In 2025 International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF) (pp. 1-12). IEEE.

Thirupathi, L., Akshaya, B., Reddy, P. C., Harsha, S. S., & Reddy, E. S. (2025). Integration of AI and Quantum Computing in Cyber Security. In Integration of AI, Quantum Computing, and Semiconductor Technology (pp. 29-56). IGI Global.

Thirupathi, L., Akshaya, B., Reddy, P. C., Harsha, S. S., & Reddy, E. S. (2025). Integration of AI and Quantum Computing in Cyber Security. In Integration of AI, Quantum Computing, and Semiconductor Technology (pp. 29-56). IGI Global.

Vadisetty, R., & Polamarasetti, A. (2024, November). Quantum Computing For Cryptographic Security With Artificial Intelligence. In 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA) (pp. 252-260). IEEE.

X. Ji, J. Dong, T. Deng, P. Zhang, J. Hua and F. Xiao, "HI-Kyber: A Novel High-Performance Implementation Scheme of Kyber Based on GPU," in IEEE Transactions on Parallel and Distributed Systems, vol. 35, no. 6, pp. 877-891, June 2024, doi: 10.1109/TPDS.2024.3379734.

Y. Lee et al., "An Efficient Hardware/Software Co-Design for FALCON on Low-End Embedded Systems," in IEEE Access, vol. 12, pp. 57947-57958, 2024, doi: 10.1109/ACCESS.2024.3387489.

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Di Pietro, R., & Erbad, A. (2023). A survey and comparison of post-quantum and quantum blockchains. IEEE Communications Surveys & Tutorials, 26(2), 967-1002.

Yavuz, A. A., Nouma, S. E., Hoang, T., Earl, D., & Packard, S. (2022, December). Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era. In 2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 29-38). IEEE

Yi, H. (2023). Machine learning method with applications in hardware security of post-quantum cryptography. Journal of Grid Computing, 21(2), 19.