

Quantum Sentinel Framework: Machine Learning-Based Detection and Mitigation of Quantum-Vulnerable Cryptography

Sultan Mesfer Aldossary

s.alossary@psau.edu.sa

Prince Sattam Bin Abdulaziz University

Manjur Kolhar

King Faisal University

Article

Keywords: AI, certificate transparency, quantum preparedness Rating, MID-term, NEAR-term, Q-Day

Posted Date: February 27th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-8777424/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Quantum computing is a looming threat to the very security of widely recognized cryptographic techniques. More specifically, its algorithms similar to Shor will disable both RSA and ECC cryptography while the effect of security provided by symmetric methods is going to be halved. Thus, it is high time that post-quantum era preparation is done in a concerted and measured manner. The paper claims the introduction of Quantum Sentinel, which is a continuous detection, assessment, simulation, and mitigation system of quantum-vulnerable cryptography in the enterprise settings powered by AI. Quantum Sentinel makes quantum readiness practical by creating a cryptographic inventory using Certificate Transparency (CT) and optional enterprise telemetry as its sources of evidence. It then adds algorithm family, key size, certificate authority (CA) issuer, signature hash, validity window, and governance context (exposure, criticality, and data lifetime) to each endpoint. It also assesses a scenario-aware Quantum Preparedness Rating (QPR) under three adversary tiers (NEAR, MID, QDAY) to measure readiness on a unified scale. On the basis of a CT-derived TLS dataset from Saudi Arabia containing 1,241 internet-facing endpoints, the public-key ecosystem observed continues to be overwhelmingly occupied by quantum-vulnerable primitives (RSA 74.4%, ECC 25.6%). In addition, the distribution of certificate issuance is very much concentrated with a few providers (Let's Encrypt 46.17%, DigiCert 17.49%, Sectigo 13.05%, Google Trust Services 8.62%). The resulting averages of organizational preparedness are low and worsened with stronger adversary assumptions (Mean QPR_NEAR 33.63, QPR_MID 18.55, QPR_QDAY 13.63). An AI threat-intelligence pipeline (Logistic Regression and Random Forest) can identify high-risk assets with high accuracy (Random Forest: Accuracy 0.9946, F1 0.9958, ROC-AUC 1.0), and the explainability aspect of it points to key size and algorithm as the most important features.

1. Introduction

The paper presents Quantum Sentinel, a forward-looking, AI-enabled system for evaluating and eradicating quantum threats. The application of Quantum Sentinel uses artificial intelligence techniques with specialized quantum threat modeling for the purpose of paving the way for organizations in the post-quantum era. The framework targets the ongoing detection of failure in cryptographic systems, estimating the organization's risk level to quantum attacks, and suggesting or automating the most appropriate counterstrategies before the attacks come into existence. Quantum Sentinel serves as a permanently alert guard that not only detects but also directs a quick and effective quantum threat response. It takes good practices, like the conducting of a cryptographic inventory and the developing of a migration plan and combines them with AI-based analysis and decision support. The framework utilizes a combination of machine learning and simulation which allows it to adapt to the changing nature of the threats by including the latest information regarding advances in quantum computing or new cryptanalysis techniques and modifying its recommendations accordingly. This flexibility is an important asset in an area where the threat situation, such as the development of new quantum algorithms or the improvement of adversaries' skills, can change erratically. Quantum Sentinel's strategy is aimed at making sure the organizations are not hit unprepared by the quantum revolution but rather are primed to meet it with courage and stamina.

Although quantum-resistant encryption development is a remarkable achievement, its further challenge that is its major deployment on a large scale [1]. Current encryption has become a crucial part of the worldwide IT infrastructure wherever it may be done, i.e. in software, hardware, client devices, and cloud servers etc [2]. Replacing these systems with new cryptography standards, they are indeed an immense project [3–4]. NIST and other agencies have pointed out that the switch to post-quantum cryptography (PQC) will be a complicated affair, and it can take as long as a decade or more for complete implementation [5–6]. For instance, in the case of upgrading the TLS protocols to support post-quantum key exchange and signatures, it would mean having to replace algorithms in all the browsers, servers, and certificate authorities all over the world [7]. Most of the post-quantum algorithms also come with a downside, i.e. the trade-offs which include bigger key sizes and signatures, higher computational power required and of course the issue of compatibility with the old systems [8]. The testing which was conducted by the organizations have revealed that PQC might increase the performance overheads with symptoms like the handshakes getting slower and the certificates needing more bandwidth and the devices not being able to function properly that are not designed for large cryptographic data [9–10]. All these operational hurdles are clear that the mere availability of the standards is not a guarantee for the immediate security, but the thorough planning and engineering are the ones that will secure the smooth transition to the PQC without disturbing the current applications [11].

The migration to post-quantum cryptography and the corresponding readiness of the organization are both important factors [12]. Quantum threats come as a surprise and even awareness of these is far from full preparation in many industries [13]. For example, an ISACA global poll of 2025 showed that while 62% of the security professionals were concerned about the influence of quantum computing, only 5% gave it the status of a top priority in their present planning and likewise, 5% had created a quantum security roadmap [14]. At the time of the survey, almost half of the respondents did not know of NIST's PQC standards. Likewise, in a huge survey involving 1,500 cybersecurity experts from the U.S. and Europe, it was reported that a staggering 91% of companies did not even have a formal plan or a roadmap for the transition to PQC. In the same study, 81% admitted that their current cryptographic setup that included libraries and hardware security modules could not cope with PQC [15]. This portrays a huge disparity between the knowledge of things and the actual readiness. There are several reasons that have led to such a huge gap, such as lack of clarity about which algorithms will be chosen, worries about the degree of interoperability and the impact on performance, and the complication that comes with having to manage an entire company's cryptographic change. Many organizations, however, continue to be unprepared to counter the quantum threats even when they are clearly warned. Experts caution that the gap in quantum readiness may lead to a future hasty and error-prone transition that is reminiscent of the Y2K remediation effort but with a more significant impact [16].

The urgency of the matter, as suggested by all these elements, clearly implies the necessity of a proactive strategy to close the quantum security gap. It will be too late to react only after the quantum computers are available (or when the attackers start using them openly). It is, therefore, a matter of putting up defenses before the imminent quantum threat materializes, indeed. The recent consensus in the cybersecurity world is that the security posture must be shifted from reactive to quantum-ready proactive. This translates into figuring out our weaknesses in encryption, knowing how and when quantum intrusions would come through our defenses, and then coming up with a plan for risk reductions beforehand. Some recent research activities have taken steps in this

direction already. For instance [17], put forward a detailed quantum security risk assessment framework considering every phase pre-migration, during-migration, and post-migration down to the algorithm, certificate, and protocol levels. Their framework correlates the detected vulnerabilities with a classical threat model (STRIDE) for impact assessment and proposes countermeasures for each phase of the PQC transition. This type of academic research contributes to the view that systematic quantum risk assessment and management are not only feasible but also essential.

This article presents Quantum Sentinel, an AI-based framework that is proactive and it helps the quantum threat assessment and mitigation process. Quantum Sentinel's aim is to provide support in the post-quantum era by merging the potential of artificial intelligence technology with the specific field of quantum threat modeling. The framework's vision is to unceasingly spot the weaknesses in cryptography, assess how much an organization is exposed to quantum-enabled attacks, and suggest or automate the best way to counteract such attacks before they take place. Quantum Sentinel is like a real watchdog that sees quantum threats coming and helps the organization respond quickly and correctly. It leverages well-known practices like keeping a cryptographic inventory and planning migrations in an agile way but at the same time applies AI for analysis and helps in decision making. The framework transforms the combination of machine learning and simulation into an ability that can easily adapt to changing threats by bringing in the current data regarding quantum computer breakthroughs or new cryptanalytic methods and changing its recommendation if needed. This feature gives a big competitive edge in a domain where the threat landscape comprising advancements in quantum algorithms and the capabilities of adversaries can unpredictably change. The strategy of Quantum Sentinel that is constantly looking ahead is meant to guarantee the organization's readiness for the quantum revolution and their ability to react with certainty and strength.

The Quantum Sentinel is a system made up of three integrated elements that together give a complete quantum cybersecurity readiness.

1.1. AI-Powered Threat Intelligence Module

This component makes use of deep learning for the purpose of constant analysis of the internal security telemetry such as configurations, logs, network traffic, and code repositories by continuous learning and thus it analyzes the external threat intelligence as well. It discerns the cryptographic vulnerabilities that are relevant to the quantum threats where the weaknesses include the RSA or ECC dependencies and the outdated TLS settings that have been done for the times which are already gone, and it ranks the weak points based on how accessible they are for being exploited and on what is the timeline for the expected quantum capabilities.

1.2. Quantum Attack Simulation

The engine of the simulator mimics the possible attacks that would be conducted by quantum-enabled users and does this using algorithm like Shor's and Grover's that are already proven. The analysis by scenarios tells the quantum adversaries' influence over the current cryptographic assets, thus making it easier to do protocol stress testing and to carry out the risk prioritization based on evidence.

1.3. PQC Transition Supports Component

The cryptographic inventory of the post-quantum migration is performed by the PQC Transition Supports component through the assessment of the cryptographic inventory of the post-quantum migration, evaluating compatibility with quantum-safe coding and recommending standardized quantum-resistant alternatives, for instance, CRYSTALS-Kyber, CRYSTALS-Dilithium. This also involves a structured transition process that aims to eliminate uncertainty, speed up deployment, and reduce disruptions in operations.

Combining these three elements, Quantum Sentinel provides a full and constant quantum security posture for the organizations. It does not just function as a one-off evaluation or temporary means, but rather an intelligent structure that is continuously learning and evolving. With the help of quantum research, the AI-driven threat intelligence updates risk assessments and automatically adjusts the mitigation recommendations as the IT systems of the organization evolve. This non-stop feedback loop not only keeps quantum readiness in line with new realities but also helps to lessen the exposure period. The new cybersecurity approach was a shift from the previous method of incident-triggered vulnerability patching to system hardening in anticipation of quantum attacks. The enterprises that adopt Quantum Sentinel can predict their "Q-day" risks several years ahead, which will allow them to prevent the critical data and infrastructure from being at risk due to quantum threats. The model that quantum sentinel utilizes not only secures the confidentiality and integrity of data against future threats but also strives to give customers and stakeholders the indication of the data resilience against attacks. Furthermore, the insights that intelligent systems yield, like a risk index with the most quantum-vulnerable assets, can aid in high-level decision-making and compliance processes, keeping the management informed and engaged in strategic risk control. Quantum Sentinel is characterized as a core component of an organization's long-term cyber defense and is like the role of intrusion detection or threat intelligence platforms, only it caters to the distinctive issues posed by the quantum era specifically.

This paper continues with the following sections: Section 2 discusses quantum computing threats and analyzes the work done in post-quantum cryptography and quantum risk assessment. It reviews related work in Section 2. Section 3 of the paper talks about the framework, Architecture of the Quantum Sentinel, which consists of AI models, a simulation environment, and integration points in an enterprise network. The framework's case study and experimental results are presented in Section 4, where it is shown how Quantum Sentinel reveals weaknesses and leads a hypothetical organization through a PQC transition. Section 5 mentions the considerations for implementation, limitations, and ways the framework could be utilized in real life. To sum up, Section 6 contains our findings, suggestions for organizations that wish to be quantum ready, and the outline of future research areas in the AI-assisted quantum cybersecurity.

2. Literature Review

The cryptographic algorithms that modern digital security is based on, have, so far, been practically impossible to break with classical computing power. But the rise of quantum computing indeed brings the security framework down like a house of cards. To be more specific, quantum computers rely on the principles of quantum mechanics to solve certain mathematical problems with speed that is exponentially higher than that of classical computers. The two quantum algorithms, i.e., Shor's algorithm and Grover's algorithm, are the ones that pose the most significant threat to encryption practices that we have today. Shor's algorithm is able, in no time at all, to factorize large numbers and compute discrete logs, thus making public-key cryptography like RSA and ECC depending on math, unsuitable for practical use. Grover's algorithm, on the other hand, gives the process of brute-force search a huge acceleration so that the strength of symmetric-key ciphers is effectively cut in half (one gets the chance to discover the key twice as fast as with classical methods). To put it simply, a quantum computer that is very powerful and uses Shor's algorithm could decrypt RSA and ECC-encrypted data, while the one using Grover could make a 256-bit symmetric key have the same security as a 128-bit one. Therefore, the large-scale quantum attacks would not only compromise the programs but also the data that are now protected with cryptographic methods.

The authors put forward an MPC-QNC architecture that combined secure computation, Physical QKD, NIST PQC, AI/ML, and hardware acceleration, thus facilitating rapid, quantum-safe distributed computations for PKI and federated ML applications. The authors presented not only quantum-safe but also breach-resilient cybersecurity services that were characterized by increased resiliency, and efficiency, and introduced MPC-QNC into HDQPKI for dispersed post-quantum PKI and TPQ-ML for secure and privacy-preserving federated learning [18].

Current-day computational security based upon digital techniques heavily depends on cryptographic algorithms which cannot be bothered by the classical computing power of the present era [19]. But the birth of quantum computers puts a big question mark on this entire security setup as to its continuance [20]. That is, the new-age quantum computers take over the traditional ones using their quantum mechanical attributes in treating some mathematical problems. In this way, they gain exponential speed-ups over classical computers. Possessing such great capabilities, the two quantum algorithms, Shor's, and Grover's, among others, become the biggest threats to the current cryptographic techniques [21]. Shor's algorithm factors large integers and computes discrete logarithms with ease, thereby compromising the math behind many popular public-key systems, namely, RSA, and ECC. On the contrary, Grover's algorithm quickens the brute-force search multiplication-wise and thus lets one discover the key quicker than the classical brute force method but at the price of a weaker cipher; hence, the ciphers become only half as strong as they possess. To illustrate the point, an adequately strong quantum computer running Shor's algorithm would be able to break the RSA and ECC encryption, whereas the Grover's algorithm would cut down the security offered by a 256-bit symmetric key to that of a 128-bit key. This means that a large number of cryptographic protocols, which are presently protecting data, would be rendered insecure due to quantum attacks on such massive scales. The repercussions of this breakdown could be big. Almost all secure digital communications and data safeguarding techniques rely on quantum attack susceptible algorithms.

The public-key cryptosystems such as RSA, ECC, and Diffie-Hellman are the support pillars of the protocols including TLS that secures HTTPS web traffic besides various applications like VPN, SSH connection, digital signatures etc. In the event of these cryptosystems falling, a huge number of transactions and communications would be exposed to the risks of not being kept secret and not authenticated. Symmetric encryption algorithms like AES are still not completely broken with the help of quantum methods but they would need majorly increased key sizes to sustain their intended security level. Thus, the rise of quantum computing is indeed a danger to the security assurances given and the current cryptographic infrastructure that supports the technological part of society. This so-called "cryptographic apocalypse" is not a hypothetical scenario but rather a very likely event considering the continuous progress in quantum research.

At the moment, quantum computers are not able to run Shor's algorithm for RSA-2048 or breaking AES-256. The quantum processors of today are still working with a few hundred noisy qubits, which is far less than the thousands or millions of fault-tolerant qubits needed to break strong encryption. The date for such computational power being available is still the topic of substantial research and discussion. A lot of the specialists are saying that the quantum computers that could crack the current encryption standards might appear in the next 10 to 20 years, an event that is often called "Q-Day" (the quantum day). Some predictions are even more daring; for instance, a RAND Corporation study mentioned by NIST talks about a breakthrough happening within a decade if the most favorable conditions are considered. More than that, recent studies have accelerated the predicted time frame by suggesting that the required qubits to decrypt RSA-2048 may be fewer than thought before—possibly a few hundred thousand noisy qubits functioning for several days, instead of millions of error-free ones—thus paving the way for RSA being insecure as early as the 2030s. The exact point of time for "Q-Day" is still in question, but there is a strong agreement that it will come while the current encryption methods are still in use. Therefore, there is an immediate requirement to set up the cryptographic protections.

The potential risk of quantum computing is not just something to worry about in the future; on the contrary, it is something we must deal with already because of the deliberate actions of the enemies. According to reports, state and non-state actors, who have a lot of resources, are amassing encrypted data with the hope of being able to decrypt it once quantum computing becomes a reality. This practice, known as "harvest now, decrypt later" (HNDL), is a stealthy, long-term intrusion that does not produce immediate signs of its occurrence. Although encrypted files and communications captured today may not be accessible for many years, they would be quickly decrypted if adversaries were to acquire quantum computers. Data that need to be kept secret for a long time, such as government archives, military communication, private medical and financial information, patents, etc., is the most at risk. These kinds of data usually need the security of several decades, thus they have to be protected by encryption that is immune to future risks. One example of this is the privacy of medical records, which is usually required for at least ten years, while government papers subject to classification may be kept under wraps for over twenty-five years. If the data is protected using RSA or ECC techniques today, the attackers who possess the copies now could probably break them in the 2030s, thus negating the covering of security for decades. The conjunction of an unavoidable quantum computing "breaking point" and the HNDL A threat is posing an extremely high risk to the current cryptographic systems.

Because of the impending risk of quantum computing, the cybersecurity sector has already started to get together and coordinate their activities. One such activity is the Post-Quantum Cryptography (PQC) project which aims to create cryptographic methods specifically resistant to quantum computers. In the

past few years, the joint efforts of researchers from learning institutions, business, and government have resulted in the selection of the quantum-resistant algorithms, their rigorous analysis, and also not to mention, considerable mathematical methods used to determine their robustness against attacks from quantum computers, such as lattice problems, hash-based constructions, and multivariate equations. The NIST (U.S. National Institute of Standards and Technology) has been the leading force behind the global effort in standardizing the PQC algorithms. The initiative started in 2016, and several submissions have been evaluated over the years, leading to the finalists being announced in 2022, among which are the CRYSTALS-Kyber algorithm for encryption and key exchange and CRYSTALS-Dilithium for digital signatures. A set of PQC standards officially approved was released by NIST in August 2024 containing traditionally accepted algorithms and guidelines for implementation globally. The security of the algorithms is based on computationally hard problems, such as the lattice problems that are not efficiently solvable by quantum algorithms, which are akin to Shor's and Grover's thus the re-establishment of security in a quantum-capable environment is aimed at.

The issue of large-scale deployment poses a greater challenge despite the fact that the development of quantum-resistant encryption is a major milestone. The modern day encryption is tightly woven into the global IT infrastructure that includes the software, hardware, client devices and cloud servers. The process of migrating these systems to the new cryptographic standards is a tremendous task. NIST and other similar organizations have pointed out the complexity and timing of the transition to post-quantum cryptography (PQC), which might well take a decade or even more for full implementation. For instance, the upgrading of the various protocols like TLS to post-quantum key exchange and signatures requires the concurrent replacement of algorithms in the different locations such as browsers, servers and certificate authorities and thus has to happen everywhere). Some of the post-quantum algorithms have introduced the need for larger keys and signature lengths as well as more demanding computations and systems compatibility issues with older versions of software. Some early trials in organizations have revealed that PQC will add to the current performance overheads, such as longer handshakes and the need for certificates that consume more bandwidth and the occurrence of errors in devices that are not intended to handle large amounts of cryptographic material. These operational difficulties imply that simply having standards is not enough to provide security right away; a thorough planning and engineering process is required to ensure that there is no disruption of existing applications during the transition to quantum-resistant methods.

One of the main questions that should be addressed is whether or not organizations are ready for the switch to post-quantum cryptography. A recent survey of the industry has shown that quantum threats awareness and preparedness are still lacking in many sectors. The ISACA pandemic poll conducted in 2025 is a case in point that illustrates this situation; it showed, amongst other things, that even though 62% of the security professionals were worried about the impact of quantum computing, merely 5% regarded it as a top priority in the present planning, and only 5% had mapped out a quantum security plan. At the time of the survey, almost half of the respondents did not know anything about NIST's post-quantum cryptography (PQC) standards. In the same manner, a big generalization of 1,500 cybersecurity practitioners working in the U.S. and Europe found that 91% of the organizations had no formal plan or roadmap for PQC transition. The same survey also revealed that 81% of the practitioners admitted that their present cryptography infrastructure, including libraries and hardware security modules, was not PQC-compatible, thereby pointing to the gap between the knowledge and the lack of preparedness in the practical sense. Among the factors delaying progress are the confusion over which algorithms to choose, the worry about the compatibility and performance issues, and the difficulty of overseeing a company-wide cryptographic change. In spite of the unambiguous alerts about the quantum threats, most organizations have not properly planned their defenses. The quantum readiness gap could lead to a future scenario where response is rushed and fraught with errors, a situation that experts liken to the Y2K remediation effort, but with much higher stakes involved.

The outlined factors are a clear signal for a strategy capable of closing the quantum security gap to be immediately developed and implemented. It would be too late to establish security measures only when quantum computers can be used by adversaries or when they actually use them for their attacks. The installing of defense against potential quantum threats has to occur before the threats ever materialize. This is the leading thought in the cybersecurity industry where the companies are expected to change their stance from being reactive to being proactive, enforcing the quantum-ready posture. Being proactive requires companies to pinpoint their cryptographic vulnerabilities, think of the timing and quantum attacks' impact and draw a roadmap for the mitigating of risks that are associated. Latest studies have positive outcomes in large part. For example [17], propose a quantum security risk assessment framework that analyses the weaknesses at the algorithm, certificate, and protocol levels during the pre-migration, migration, and post-migration phases. The framework links the identified vulnerabilities to the classical STRIDE threat model to evaluate the impact and offers recommendations for each stage of the PQC transition. This study illustrates the fact that the quantum risks may be assessed and managed systematically which is also a point hard to reach given the modern networks' complexity and the threats with their changing nature.

The researchers [22] suggested a smart mixed cryptographic system for IoT gadgets which combined lightweight primitives, chaotic systems, and quantum-resistant methods. Outputs (MSE, MAE, PSNR, SSIM) indicated powerful encryption, slight distortion, low energy (3.536 μ J) consumption, and being resistant to both cryptanalytic and quantum attacks. The authors [23], put into practice the combination of QKD-PQC communication system with the dynamic obfuscation of the operation sequences/parameters and the GPS-free quantum synchronization. The results showed that the performance was real-time and had a small overhead, which provided stronger protection against practical attacks and the ability to adapt to future threats. The researchers recommended the combined utilization of an AI-based cybersecurity framework with LSTM based anomaly detection, secured SHA-256 homomorphic hashing for integrity verification, Q-learning for automated response, and LWE lattice-based encryption for post-quantum security. The results obtained through simulation accurately indicated the performance of the proposed framework's features: detection of anomalies with high precision, recognition of tampering with great reliability, threat management that adapts to the situation, and the provision of autonomous protection that is scalable for IoT infrastructures [24]. In [25], recommended a healthcare data-sharing scheme for HIE that was post-quantum core secure and would use the XMSS signatures together with the consortium blockchain to make sure the EMR had integrity, authenticity and could be traced. Moreover, they incorporated AI-assisted diagnosis generation. Security analysis established resilience to attacks, and the experiments indicated about 49% less computational overhead and approximately 36% less blockchain storage in comparison with the existing schemes. The researchers [26], have put forward a quantum-classical mixed IoT security scheme that includes QKD, PQC, and quantum machine learning to enhance anomaly detection, encryption, and predictive maintenance. The tests on NISQ/IBM simulators had 98.7% detection accuracy, 80% reduction in latency, and 3.9% false positives. The method also raised federated learning

accuracy (14.5%), increased secure key rate (500%), cut down training time (50%), and doubled energy efficiency (225%), which makes it possible to have large-scale real-time quantum-secured IoT applications. In their paper [27], the authors introduced a deepfake prevention framework that encompasses technical and governance-based countermeasures. The preventive framework comprised trusted content assurance, detection/monitoring, awareness with human-in-the-loop verification, and policy/regulation. It utilized a combination of watermarking, blockchain, and digital signatures, and it was found that Falcon-512 was the most efficient post-quantum DSA with lower resource use and gas costs in the comparison of classical vs post-quantum DSAs, thus allowing for real-time quantum-resilient media authenticity and traceability. The authors presented a hybrid IoT security framework that leveraged post-quantum cryptography (lattice, hash, and code-based schemes) together with deep learning intrusion detection to counter both classical and quantum attacks. They tuned lightweight PQC for edge/IoT devices with limited resources and allowed the IDS to learn adaptively for new threats. The simulation results demonstrated the effectiveness of the system with 12.5 ms for key generation, 25.3 ms for encryption/decryption, 18.7 ms for latency, 5000 ops/sec for throughput, and 2.4 mJ for energy consumption [28]. The rresearchers have systematically evaluated the performances of PQC algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+) for IoT/edge cryptographic scheduling, under different loads, and measured various parameters like encryption/decryption time, latency, execution speed, energy efficiency, and scalability. The performance results revealed that among all three, CRYSTALS-Kyber was the best, in terms of overall efficiency, with the smallest delays and power use, and at the same time maintaining quantum resistance. Besides, the authors also recommended a dynamic cryptographic scheduling method that would ultimately lead to optimization of security levels as well as resource allocation in large-scale IoT deployments [29].

Table 1 provides a summary of the latest developments in PQC and quantum-resilient security measures for IoT and IoMT contexts. The research reveals a major trend of combining PQC with modern techniques, such as light cryptography, chaos-based encryption, blockchain, QKD, and AI/ML-based intrusion detection, among others. Some of the proposals have been able to achieve impressive security levels and performance, but, on the whole, most of the methods have difficulties implementing, as they are demanding in terms of computational power and scalability. Moreover, quantum solutions are still very much dependent on the capabilities of the NISQ devices which makes it difficult to deploy them in the real world. The table, therefore, points to the need for future research to develop lightweight, scalable, and adaptable PQC-enabled frameworks that can support various IoT infrastructures with limited resources.

Table 1
Comparison of recent PCQ security approaches for IoT/IoMT systems, highlighting employed technologies, key weaknesses, and proposed mitigation solutions.

Ref	Technology / Approach	Weaknesses (few words)
[22]	Hybrid cryptosystem for IoMT (lightweight crypto + chaos + PQC)	Limited real-world validation
[23]	Integrated QKD–PQC with dynamic obfuscation + GPS-free synchronization	Implementation cost/complexity
[24]	AI cybersecurity (LSTM anomaly + salted SHA-256 hashing + Q-learning + LWE)	High compute demand
[25]	Post-quantum HIE scheme (XMSS + consortium blockchain + AI diagnosis)	Blockchain scalability constraints
[26]	Quantum–classical IoT security (QKD + PQC + QML + QFL)	Depends on NISQ limitations
[27]	Deepfake prevention (watermarking + blockchain + PQC DSA Falcon-512 + governance)	Adoption and compliance challenges
[28]	Hybrid PQC + deep learning IDS for IoT (lattice/hash/code crypto)	IDS false alarms risk
[29]	PQC performance evaluation + dynamic cryptographic scheduling (Kyber best)	Limited adaptability to heterogeneous IoT

3. Proposed Quantum Sentinel Framework

The flowchart of the Quantum Sentinel architecture, depicted in Fig. 1, shows that it operates as a closed-loop pipeline as shown in the Algorithm 1.1. The whole procedure starts at the input data layer, where the reality of the organization’s operational environment is confirmed by the collection of cryptographic evidence. The proposed architecture uses two sets of inputs that are mutually reinforcing. The first input set is internet-facing exposure intelligence, which comes from the Certificate Transparency logs. These logs contain the tamper-proof issuance records of the TLS certificates, which allows the framework to monitor the public-key algorithms, algorithms and key size issuers, signature hash function's period, and the validity period on public endpoints. The second input set is enterprise telemetry, which consists of internal observations like PKI repositories, certificate stores, VPN and gateway configurations, application configurations, and security logs. All these input sources together lead to reduced blind spots: Certificate Transparency logs disclose assets that are visible to the outside world, while enterprise telemetry gives a view into the internal setup.

The cryptographic inventory component of the system is responsible for all the evidence that is ingested and it acts as the normalization and structuring layer of the whole system. The main purpose of the component is to turn the unprocessed certificate and configuration observations into a uniform, asset-based representation that allows reasoning throughout the system. Every endpoint or system is linked to a uniform record that contains the identifiers (asset_id, asset_name), the operational context (service category, exposure level, protocol), and the cryptographic attributes (primitive type, algorithm family, key size, issuer, signature hash, validity window). This inventory stage acts not only as a database but also as the center of feature engineering. The module extracts normalized fields such as “alg_norm” (for instance, RSA versus ECC) and produces structured inputs for both machine learning models and scenario-based risk scoring. Therefore, this component converts cryptographic deployments into features that can be consumed by machines and guarantees consistency among different data sources.

The AI threat intelligence component processes the inventory to create predictive triage. Its main task is to find and rank quantum-relevant vulnerabilities over a scale, not relying on manual review or static rule-based methods. In practice, quantum exposure is treated as a classification problem where supervised machine learning forecasts the likelihood of an asset being in a high-risk group. Logistic Regression ensures clear and compliance-friendly

decision margins, whereas Random Forest models can detect intricate, non-linear interactions among factors like algorithm family, key size, issuer patterns, and hash functions. The module then produces a probability score that aids in the process of ranking and automated prioritization. Moreover, the design brings out the concept of explainability: the importance and attribution of features can be drawn out to indicate which cryptographic features affected the risk prediction, thus being supportive of the analyst's trust and facilitating strong risk governance.

The AI threat intelligence module oversees the predictive triage by processing the inventory. Its primary role is to discover and classify vulnerabilities which are of concern to the quantum world, but it does this without the need for a manual review or static rule-based methods. More specifically, quantum exposure is viewed as a classification problem where supervised machine learning predicts the chance of the asset being placed in the high-risk group. On the one hand, Logistic Regression gives unambiguous and compliance-friendly decision margins, while on the other hand, Random Forest models can recognize complex, non-linear interactions among various factors such as algorithm family, key size, issuer patterns, and hash functions. After that, the module gives out a probability score, which is used in the process of ranking and automatic prioritization. In addition, the design puts the aspect of explainability into the light: the significance and attribution of features can be manipulated to show which cryptographic features influenced the risk prediction, thereby winning the trust of the analyst and enabling robust risk governance.

The component of the post-quantum mitigation plan transforms QPR-ranked results into practical measures and a detailed transition roadmap. This way, the issue of not reducing the risks identified is tackled. The order of importance is set according to the asset, type of service, and exposure, with the module giving levels (P0, P1, or P2) and putting the assets in the migration waves that are divided by phases. The recommended controls are directed towards hybrid and post-quantum cryptographic mechanisms so that interoperability can be assured and quantum-related risks can be reduced to the minimum. In the case of TLS, this generally means hybrid key establishment where the classical ECDHE is combined with a post-quantum cryptographic key encapsulation mechanism like Kyber, and post-quantum signature schemes such as Dilithium are used gradually as the situation allows. The module, in addition, looks into the issue of deployment feasibility and spots possible compatibility problems that may arise due to factors such as larger keys or certificates, lack of client support, or PKI integration. The mitigation plan is made up of a task list organized by priority and a strategy for sequencing, which makes it possible for organizations to take care of the most critical and exposed services first and then schedule future upgrades for internal or lower-risk systems.

The Quantum Sentinel deployment and continuous operation take place in the enterprise network block environment. The system is designed to work with the operational processes and not just as a one-off evaluation. In reality, the inventory layer keeps being updated when certificates are rotated and services changed, the threat intelligence models trained anew when new data and labeling strategies come up, and the QPR engine recalibrated at regular intervals to check the readiness trend. This looped architecture allows Quantum Sentinel to continue supporting the governance of crypto-agility by constantly observing the cryptographic posture, predicting and prioritizing quantum risk, validating threats through quantum attack models, quantifying readiness in a scenario-specific way, and then giving migration guidance that reduces risk through a controlled, slowed-down approach.

Algorithm 1.1

Quantum Sentinel data pipe line.

Algorithm 1: QUANTUM-SENTINEL(CT_Data, Enterprise_Telemetry, Tiers) Input: CT_Data (TLS certificates), Enterprise_Telemetry (optional), Tiers = {NEAR, MID, QDAY} Output: Scored_Inventory, Ranked_Assets, AI_Predictions, Mitigation_Plan, Post_Mitigation_Scores
1: Raw_Data = INGEST(CT_Data, Enterprise_Telemetry)
2: Inventory =NORMALIZE_TO_ASSET_SCHEMA(Raw_Data)
3: Inventory = ENRICH_FEATURES(Inventory) // Extract: algorithm, key_size, issuer, signature_hash // Derive: agency, exposure, criticality, data_lifetime
4: for each asset Ai in Inventory do
5: Fi =QUANTUM_FRAGILITY(Ai.algorithm)
6: Ki = KEY_PENALTY(Ai.algorithm, Ai.key_size)
7: Ei = EXPOSURE_WEIGHT(Ai.exposure)
8: Ci = CRITICALITY_FACTOR(Ai.criticality)
9: Li = LIFETIME_FACTOR(Ai.data_lifetime_years)
10: for each tier t in Tiers do
11: lit = TIER_IMPACT(Ai.algorithm, t)
12: end for
13: Ri = RISK_SCORE(Fi, Ki, Ei, Ci, Li, li,QDAY)
14: for each tier t in Tiers do
15: QPRit = QPR_SCORE(Ri, lit)
16: end for
17: end for
18: Ranked_Assets = SORT_BY_RISK(Inventory)
19: AI_Model = TRAIN_AI_THREAT_INTEL(Inventory)
20: AI_Predictions = PREDICT_RISK(AI_Model, Inventory)
21: Attack_Sim_Output = QUANTUM_ATTACK_SIMULATION() // Shor PoC + Grover PoC
22: Mitigation_Plan = GENERATE_MITIGATION_PLAN(Ranked_Assets)
23: Inventory_Post = APPLY_MITIGATION_SIMULATION (Inventory, Mitigation_Plan)
24: Post_Mitigation_Scores = RECOMPUTE_QPR(Inventory_Post)
25: return Inventory, Ranked_Assets, AI_Predictions, Mitigation_Plan, Post_Mitigation_Scores

4. Dataset

Quantum Sentinel was provided with data that was generated through a meticulous procedure that switched over the physical-world cryptographic evidence to an enterprise inventory that was fit for quantum risk assessment and post-quantum transition planning. Among other things, the data was entirely based on Certificate Transparency (CT), which is a global system of public logs that keep track of the issuance of TLS/SSL certificates. CT logs are the most trustworthy evidence of cryptographic operations on the internet and at the same time make it possible, through a non-intrusive method, to monitor on a large scale the real cryptographic practices without the need of internal access to the organization's infrastructure. The CT logs of Saudi Arabia were the focus of the research, with special emphasis on public sector suffixes like ".gov.sa", which are believed to be the most significant areas for enterprise and governmental deployments. Certificate data was extracted utilizing CT indexing services, such as crt.sh, which offer a query-accessible interface to certificate records. To obtain certificate entries, queries were performed employing domain patterns (e.g., %.gov.sa), and after that, the raw records were processed to get the basic certificate attributes such as domain name (Common Name and Subject Alternative Names), issuer distinguished name (certificate authority/provider), validity timestamps (notBefore, notAfter), public-key algorithm type, key size, and signature hash algorithm. Because CT logs contain redundant entries, deduplication was applied to get rid of duplicate certificate observations. The process of duplicate removal was done with the use of certificate identifiers (e.g., crt.sh certificate ID) and repeated domain instances to make sure that every TLS endpoint was represented in a consistent manner. After the extraction process, the CT data was standardized into a corporate-level cryptographic inventory format, where each detected TLS end point was considered a security asset. The assets were given unique IDs (for example, SA-1, SA-2) and were organized in a table-like structure that had the

following attributes: asset name, protocol context (TLS), exposure class (public-facing), and cryptographic primitive type (public-key). This normalization process guaranteed that Quantum Sentinel's subsequent modules, such as AI-based threat prediction, quantum preparedness rating (QPR), and mitigation planning, would be compatible. To facilitate higher-level grouping and sector risk analysis, further computed attributes were added, such as suffix categorization and agency extraction (for instance, mapping the subdomains to their main government agency domain like moe.gov.sa).

The dataset for quantum risk modeling was further enriched with contextual attributes-like the assumed data confidentiality lifetime (in years) and asset-criticality values- thus allowing the framework to take into account the "harvest-now, decrypt-later" situation in scoring. Lastly, Quantum Sentinel calculated scenario-based quantum impact parameters (NEAR, MID, QDAY), composite risk scores, and preparedness metrics (QPR), thereby generating a fully scored dataset that was ranked, reported, and experimentally evaluated. The enriched and scored dataset was exported into reproducible CSV outputs as a means of ensuring transparency and facilitating future re-analysis.

The engine of the QPR stands as the pivotal element of Quantum Sentinel for decision-making and measurement. It combines different data sources like structured inventory data, AI-powered prioritization signals, and scenario-based quantum impact assumptions to produce a single preparedness score. The engine is based on the view that quantum threats are not only dependent on time but also on capabilities, and thus it measures preparedness in different layers, such as near-term, mid-term, and Q-day conditions, instead of assuming one static enemy. The engine evaluates the quantum vulnerability for each asset, which is defined as the susceptibility of the underlying cryptographic primitive to Shor or Grover class attacks; applies cryptographic strength penalties, like key-size sensitivity in public-key systems; performs exposure weighting, where public endpoints are assigned higher urgency; assesses data lifetime sensitivity, which increases urgency for assets requiring long-term confidentiality due to the harvest-now-decrypt-later risk; and judges asset criticality, reflecting business impact. These elements are merged into a bounded score that results in three outputs: a preparedness value per asset, a sorted list of the most urgent security gaps, and an organization-level readiness summary that can be tracked over time. The QPR engine also allows the measurement of advancements made from mitigation efforts since the scoring process can be repeated after system changes.

5. Results

Quantum Sentinel's main goal is to simplify the process of detecting the looming threat of new cryptographic attacks by automatically mapping and labeling the quantum-susceptible deployments to the places where they are actually used in the enterprise. The methodology set forth for the accomplishment of this includes building up a cryptographic inventory through the collection of metadata related to Transport Layer Security (TLS) certificates from the logs of Certificate Transparency (CT) for Saudi domains. Every TLS endpoint is treated as a security asset whose value is increased by providing the cryptographic attributes required for the appraisal of quantum risks, these attributes are: public-key algorithm family, key size, issuer or certificate authority (CA) provider, and signature hash function. The risk that each endpoint is associated with is normalized in an asset-imposed way which gives rise to a systematic approach for recognizing which endpoints rely on cryptographic primitives that will be easily compromised under quantum adversary models, primarily those that are vulnerable to the Shor's algorithm method.

The baseline threat identification points out that the public-key ecosystem still mainly depends on classical cryptography. The distribution of algorithms, illustrated with a pie chart in Fig. 2, shows that RSA accounts for 74.4% of the total observed TLS endpoints, while ECC only occupies 25.6% as depicted in the bar chart in Fig. 3. This finding has substantial security implications because both RSA and ECC rely on the hardness of the integer factorization and the elliptic curve discrete logarithm assumptions that are vulnerable to Shor-type quantum attacks. As a result, the framework uncovers a significant gap in cryptographic safety; even though global standardization and migration to post-quantum cryptography (PQC) are already in place, real-world usage is still mostly dependent on quantum-vulnerable primitives.

Apart from the analysis of the algorithm distribution, Quantum Sentinel also performs an explicit vulnerability classification. This is done through the mapping of the observed cryptographic primitives to the different quantum vulnerability categories. The findings are reflected in Fig. 4 (Quantum-Vulnerable TLS Endpoints / Shor Exposure) where almost all endpoints are marked as quantum-vulnerable since they are using RSA or ECC and no post-quantum cryptography (PQC) applications are found in the dataset. The immediate operational insight that is provided by Fig. 4 is that the organizations having analogous cryptographic infrastructures are practically in the same boat regarding the risk of becoming victims of the future "harvest-now, decrypt-later" attacks. The latter refers to the situation where the opponents gather the encrypted traffic now and it gets decrypted once the quantum computing power is high enough.

Quantum Sentinel improves the process of making cybersecurity decisions that can be acted upon by first scoring and then ranking vulnerabilities that have been found. In Table 2 (Top Risky Endpoints), some of the very risky endpoints are shown, they are autodiscover.redf.gov.sa, auth.redf.gov.sa, and ae.moe.gov.sa. Most if not all of these endpoints are using RSA-2048 keys and have been granted certificates from leading certification authorities like DigiCert. The reason for identifying these endpoints as highly sensitive is that they grant access to authentication and email discovery services which are not only often targeted but also require long-term confidentiality sometimes. So, Objective 1 is met through the delivery of automated cryptographic discovery, algorithm-based quantum vulnerability detection, and risk-ranked threat identification aligned with quantum-era adversary models.

Table 2
Top Risky Endpoints.

asset_id	asset_name	alg_norm	key_size	risk_score	issuer
SA-12	autodiscover.redf.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-13	autodiscover.redf.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-14	auth.redf.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-15	scega.gov.sa	RSA	2048	83.0	CN=Sectigo RSA Domain Validation Secure Server CA
SA-3	ae.moe.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-4	p-hq-vm-pm-01.moe.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-5	amana-md.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-6	gispt.redsea.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-7	abherdev.redsea.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-9	complaints-cpd-uat.sama.gov.sa	RSA	2048	83.0	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
SA-1070	back.ghadah.med.sa	RSA	2048	83.0	CN=R13, O = Let's Encrypt, C = US
SA-1071	back.ghadah.med.sa	RSA	2048	83.0	CN=R13, O = Let's Encrypt, C = US

The Quantum Sentinel's third goal is to provide a quantum risk model that is not only measurable but also scenario-aware, hence organizations can easily evaluate their cryptographic readiness based on different quantum threat maturity assumptions. Rather than just identifying weak algorithms as in traditional vulnerability assessments, the Quantum Sentinel sets up a systematic readiness metric known as the Quantum Preparedness Rating (QPR) which conveys readiness on a unified 0-100 scale. Each asset's QPR is derived from a composite scoring model that takes into account the factors of cryptographic fragility, key strength penalties, exposure context, and operational sensitivity indicators. The QPR is determined at three adversarial levels (NEAR, MID, and QDAY) so that the dynamically changing nature of the quantum capabilities is captured, helping in both short-term prioritization and long-term migration planning.

The metric proposed is really scenario-based, as it is shown in Fig. 5 through the visualization of differences in preparedness among the three threat levels. The distribution shows a very clear and significant drop from NEAR to QDAY, which means that systems get less and less prepared with the increase of quantum adversary assumptions. This is mainly due to the fact that quantum-vulnerable public-key cryptographic systems like RSA and ECC, which are widely used, are the main reason for the significant reduction of threat modeling under Shor-capable. The aggregate preparedness indicators further support this point, as there is a strong decrease of means across tiers: Mean QPR_NEAR = 33.63, Mean QPR_MID = 18.55, and Mean QPR_QDAY = 13.63. These metrics not only provide a starting point for organizational preparedness but also allow the monitoring of quantum readiness trends to be done continuously.

Besides preparedness assessment, Quantum Sentinel also facilitates risk intelligence which in turn impacts governance and decision-making. The framework specifically maps out the cryptographic supply chain by looking into the issuing bodies of Transport Layer Security (TLS) certificates and the Certificate Authority (CA) providers. This examines is crucial as the post-quantum cryptography (PQC) migration plans rely on both the internal systems and the external certificate providers within the trust ecosystems. The concentration of issuers is illustrated in Fig. 6 (Top CA Providers in Dataset), which shows that most of the endpoints that were observed are issued by Let's Encrypt, followed by DigiCert, Sectigo, and Google Trust Services. The distribution table of issuers corresponding to this reveals the extent of the dominance: Let's Encrypt (46.17%), DigiCert (17.49%), Sectigo (13.05%), and Google Trust Services (8.62%). It is evident from these results that a small number of certificate providers are responsible for the majority of the TLS traffic that is being monitored, which in turn points out the significance of CA readiness and the alignment of PQC support in the planning of enterprise migrations.

To improve Quantum Sentinel's threat identification functions over and above the deterministic cryptographic checks, an AI-led threat intelligence pipeline is integrated that will automatically forecast and rank security risks relevant to quantum across the identified TLS assets. Cryptographic inventory and vulnerability mapping ascertain what algorithms are in use, but the AI module meets a complementary operational requirement by allowing for the scalable, automated triaging of vast endpoint populations and for the generation of explainable risk signals that guide security analysts toward the most critical exposures. In this regard, the component envisions threat identification as a supervised learning problem, where endpoints are cast into high-risk and low-risk classes, using enriched CT-derived cryptographic metadata.

The model's classification capability is shown in Fig. 7, which produced 129 true negatives (low-risk correctly predicted) and 237 true positives (high-risk correctly predicted), with just 7 false positives and no false negatives. This result is especially important for threat intelligence systems because false negatives mean high-risk endpoints that have not been detected. The Random Forest confusion matrix (Fig. 8) adds another layer of predictive reliability by cutting false positives to 2 but keeping perfect recall for high-risk endpoints, which is a sign of strong generalization and steady detection performance. ROC analysis supports these conclusions. Both models, as shown in Fig. 9 (ROC Curves for AI Threat Intelligence Models), have almost perfect class discrimination, each giving ROC-AUC = 1.0. The quantitative comparison in Table 2 (Model Performance Summary) validates the high accuracy of both methods, with Random Forest delivering the best compromise of precision and F1 score.

Besides predictive accuracy, Quantum Sentinel also emphasizes explainability for its use in practical security scenarios. The feature attribution analysis based on Random Forest, illustrated in Fig. 10 (Feature Importance), points out that key size is the strongest predictor whereas algorithm family indicators (RSA/ECC) and issuer-related signals are less influential, in descending order of importance.

This discovery conforms to the security principles of cryptography that are already accepted. It is a matter of RSA key lengths and methods that can be attacked by Shor's algorithm, which mainly decide about quantum fragility. The AI layer's operational usefulness is proved by the ranked outputs, where the endpoints are arranged according to the predicted probability of risk (for instance, `pred_risk_prob = 1.0`), which allows for the creation of a high-confidence and prioritized threat list for mitigation planning. The AI threat intelligence module has a significant contribution to Objective 1 by delivering threat prioritization that is scalable, comprehensible, and automated, and that is in line with the requirements of quantum security.

Together with predictive accuracy, Quantum Sentinel puts much strive on explainability in order to support its acceptance in the actual security settings. According to Fig. 9, the feature attribution analysis done through Random Forest has come to the conclusion that key size is the most important factor influencing the prediction, followed by indicators of the algorithm family (RSA/ECC) and signals related to the issuer. The conclusion is in agreement with the basic principles of cryptographic security, as the sizes of RSA keys and the primitives that can be attacked by Shor's algorithm are the main factors responsible for quantum vulnerability. The practical benefit of this AI layer is shown through the ranked outputs, where the endpoints are arranged in decreasing order of predicted risk probability (e.g., `pred_risk_prob = 1.0`), letting the generation of a high-confidence, prioritized threat list for mitigation planning. The AI threat intelligence module is a significant contributor to Objective 1 because it provides scalable, explainable and automated threat prioritization, all of which are in accordance with the quantum security requirements.

Quantum Sentinel's fourth objective is to provide post-quantum mitigation guidance that can be acted upon, as well as measuring the readiness improvement through the implementation of quantum-safe cryptographic solutions. The first three objectives focus on determining the risks and evaluating the readiness in the different scenarios, while the fourth objective is to make a transition roadmap of the post-quantum scenario based upon the findings in a structured way. The operational environment is such that post-quantum migration is carried out in phases where the most critical services are exposed and in use while at the same time the new system and the old one must be able to cooperate. Quantum Sentinel will deal with these constraints by producing the recommendations for mitigating, setting migration priorities, and doing prior and post analysis of the Quantum Preparedness Rating (QPR) to measure the progress.

The framework employs a simulated mitigation pipeline consisting of upgrading high-risk cryptographic endpoints to post-quantum or hybrid cryptographic configurations to evaluate the influence of mitigation. The risk scoring and quantum vulnerability indicators showed that 790 assets, out of 1,241, needed mitigation. These assets mostly comprise RSA public-key endpoints because, contrary to other cryptographic primitives used in the dataset, RSA is directly compromised under the assumption of a Shor-capable adversary. The primary mitigation strategy involves, for example, the combination of the classical ECDHE with a post-quantum Key Encapsulation Mechanism (KEM) like Kyber (for instance, ECDHE + Kyber768) and thus hybrid TLS key establishment. This method is in accordance with the best practices for cryptographic migration, which facilitate the introduction of post-quantum cryptography (PQC) while still allowing the existing clients to connect.

The evaluation of the correction procedure's power is that it is based on layers of readiness improvement. In all threat tiers, there is a considerable increase in preparedness represented by Table 3 (QPR Pre vs Post Mitigation Summary). The NEAR scenario is characterized by a mean QPR increase from 33.63 to 60.83 ($\Delta = 27.20$). In the MID scenario, mean QPR ascends from 18.55 to 55.83 ($\Delta = 37.28$). It is remarkable that, when considering the highest adversary tier (QDAY), preparedness goes up from 13.63 to 53.08 ($\Delta = 39.46$). This trend leads to the conclusion that quantum-safe mitigation has the broadest effect under the conditions of high-capability adversary, which is also the most critical point for classical public-key systems' vulnerability. The corresponding figure is found in Fig. 10 (Mean QPR Improvement After PQC/Hybrid Mitigation), which portrays these results in a very clear way, as the post-mitigation bars are already showing a consistent increase across NEAR, MID, and QDAY tiers. Moreover, this indicates that Quantum Sentinel contributes to the development of a measurable resilience enhancement.

Table 3
QPR Pre vs Post Mitigation Summary.

Tier	Mean QPR (Pre)	Mean QPR (Post)	Δ Improvement
NEAR	33.63	60.83	27.20
MID	18.55	55.83	37.28
QDAY	13.63	53.08	39.46

The evaluation of the correction procedure's power is that it is based on layers of readiness improvement. In all threat tiers, there is a considerable increase in preparedness represented by Table 2 (QPR Pre vs Post Mitigation Summary). The NEAR scenario is characterized by a mean QPR increase from 33.63 to 60.83 ($\Delta = 27.20$). In the MID scenario, mean QPR ascends from 18.55 to 55.83 ($\Delta = 37.28$). It is remarkable that, when considering the highest adversary tier (QDAY), preparedness goes up from 13.63 to 53.08 ($\Delta = 39.46$). This trend leads to the conclusion that quantum-safe mitigation has the broadest effect under the conditions of high-capability adversary, which is also the most critical point for classical public-key systems' vulnerability. The corresponding figure is found in Fig. 10 (Mean QPR Improvement After PQC/Hybrid Mitigation), which portrays these results in a very clear way, as the post-mitigation bars are already showing a consistent increase across NEAR, MID, and QDAY tiers. Moreover, this indicates that Quantum Sentinel contributes to the development of a measurable resilience enhancement [Refer Table 4].

Table 4
Table threat endpoints

table threat endpoints							
asset_id	asset_name	alg_norm	key_size	risk_score	issuer	signature_hash	
11	SA-12	autodiscover.redf.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
12	SA-13	autodiscover.redf.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
13	SA-14	auth.redf.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
14	SA-15	scega.gov.sa	RSA	2048	83	CN=Sectigo RSA Domain Validation Secure Server...	sha256
2	SA-3	ae.moe.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
3	SA-4	p-hq-vm-pm-01.moe.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
4	SA-5	amana-md.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
5	SA-6	gispt.redsea.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
6	SA-7	abherdev.redsea.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
8	SA-9	complaints-cpd- uat.sama.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
1069	SA-1070	back.ghadah.med.sa	RSA	2048	83	CN=R13,O = Let's Encrypt,C = US	sha256
1070	SA-1071	back.ghadah.med.sa	RSA	2048	83	CN=R13,O = Let's Encrypt,C = US	sha256
1073	SA-1074	en.elajsudair.med.sa	RSA	2048	83	CN=WR1,O=Google Trust Services,C = US	sha256
1074	SA-1075	en.elajsudair.med.sa	RSA	2048	83	CN=WR1,O=Google Trust Services,C = US	sha256
1075	SA-1076	cpanel.udh.med.sa	RSA	2048	83	CN=R12,O = Let's Encrypt,C = US	sha256
1076	SA-1077	cpanel.udh.med.sa	RSA	2048	83	CN=R12,O = Let's Encrypt,C = US	sha256
52	SA-53	complaints-cpd.sama.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
53	SA-54	complaints-cpd- uat.sama.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
55	SA-56	pif.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
25	SA-26	emtithalgrafana.mc.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
26	SA-27	vhdgds4pap01.dgda.gov.sa	RSA	2048	83	CN=Sectigo RSA Domain Validation Secure Server...	sha256
27	SA-28	vhdgds4pap01.dgda.gov.sa	RSA	2048	83	CN=Sectigo RSA Domain Validation Secure Server...	sha256
28	SA-29	autodiscover.moia.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
30	SA-31	sera.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256
31	SA-32	iamnafathstg.moe.gov.sa	RSA	2048	83	CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1,...	sha256

The second purpose of Quantum Sentinel is to check and measure the actual application of quantum-enabled cyber-attacks via a controlled simulation. Even though identification of threats could point out the weaknesses of the algorithms, such as the exposure of RSA or ECC, risk assessment that is objective requires a clearly demonstrated link between the cryptographic implementations and the quantum attack mechanisms that are capable of breaking them. Quantum Sentinel therefore employs a quantum attack simulation environment that mimics the impact of the quantum algorithms, particularly Shor's algorithm for public-key compromise and Grover's algorithm for speeding up brute-force search, via Qiskit-based circuit simulation. This feature serves two major purposes: the first is that it delivers a working proof-of-concept that shows the weakness of RSA and ECC under quantum power; the second is that it produces simulation outputs that are reproducible and thus increase the scientific rigor of the framework's quantum threat model [Refer Table 5].

Table 5
Table agency risk summary

Sl.	agency	assets	mean_risk	mean_QPR_NEAR	mean_QPR_MID	mean_QPR_QDAY	rsa_count	ecc_count
0	amana-md.gov.sa	5	83	32.75	16.5	12.75	5	0
1	amanataljouf.gov.sa	4	83	32.75	16.5	12.75	4	0
2	aseer.gov.sa	3	83	32.75	16.5	12.75	3	0
3	balady.gov.sa	2	83	32.75	16.5	12.75	2	0
4	bc.gov.sa	1	83	32.75	16.5	12.75	1	0
5	bog.gov.sa	2	83	32.75	16.5	12.75	2	0
6	clsr.gov.sa	2	83	32.75	16.5	12.75	2	0
10	dgda.gov.sa	6	83	32.75	16.5	12.75	6	0
14	fg.gov.sa	3	83	32.75	16.5	12.75	3	0
13	energy.gov.sa	1	83	32.75	16.5	12.75	1	0
11	dsc.gov.sa	1	83	32.75	16.5	12.75	1	0
23	jtc.gov.sa	1	83	32.75	16.5	12.75	1	0
24	makkah.gov.sa	1	83	32.75	16.5	12.75	1	0
25	masar.gov.sa	2	83	32.75	16.5	12.75	2	0
15	gdnc.gov.sa	1	83	32.75	16.5	12.75	1	0
16	gmedia.gov.sa	1	83	32.75	16.5	12.75	1	0
21	hrsd.gov.sa	1	83	32.75	16.5	12.75	1	0
20	hrda.gov.sa	3	83	32.75	16.5	12.75	3	0
19	holymakkah.gov.sa	2	83	32.75	16.5	12.75	2	0
26	mc.gov.sa	13	83	32.75	16.5	12.75	13	0

Owing to the fact that the presently available quantum machines are incapable of factoring large RSA key sizes (at least 2048-bits) in a practical time, the Shor's algorithm has been incorporated in a truncated version to show the same mathematical attack pathway exploited for RSA encryption. More precisely, Quantum Sentinel performs an order-finding proof-of-concept, i.e., it factors a composite integer by combining quantum period-finding with classical post-processing. The trial produces a measurement distribution from the quantum circuit, which unveils the probability peaks that are related to the hidden periodic structure. This structure is crucial for the recovery of the multiplicative order rrr . The peaks help in estimating the phase fractions by means of continued fraction expansion, and then classical greatest common divisor operations are used to obtain the non-trivial factors. The results, as depicted in Fig. 11, reveal the presence of the more frequent measurement outcomes that signify bitstrings associated with periodicity. These outcomes deliver empirical proof that the circuit indeed had access to the periodic structure that was necessary for factor extraction [Refer Table 6].

Table 6
domains in top agencies.csv

	asset_id	asset_name	agency	alg_norm	key_size	risk_score	QPR_QDAY	issuer_provider	signature_hash
4	SA-5	amana-md.gov.sa	amana-md.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
22	SA-23	amana-md.gov.sa	amana-md.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
23	SA-24	amana-md.gov.sa	amana-md.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
78	SA-79	amana-md.gov.sa	amana-md.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
80	SA-81	aseer.gov.sa	aseer.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
107	SA-108	bc.gov.sa	bc.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
127	SA-128	amanataljouf.gov.sa	amanataljouf.gov.sa	RSA	2048	83	12.75	GoDaddy	sha256
129	SA-130	amanataljouf.gov.sa	amanataljouf.gov.sa	RSA	2048	83	12.75	GoDaddy	sha256
130	SA-131	amanataljouf.gov.sa	amanataljouf.gov.sa	RSA	2048	83	12.75	Other	sha256
131	SA-132	amanataljouf.gov.sa	amanataljouf.gov.sa	RSA	2048	83	12.75	GoDaddy	sha256
134	SA-135	balady.gov.sa	balady.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
148	SA-149	aseer.gov.sa	aseer.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
149	SA-150	balady.gov.sa	balady.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
152	SA-153	aseer.gov.sa	aseer.gov.sa	RSA	2048	83	12.75	DigiCert	sha256
154	SA-155	amana-md.gov.sa	amana-md.gov.sa	RSA	2048	83	12.75	DigiCert	sha256

The Shor simulation has shown that the compromise chain, which puts the RSA and ECC TLS endpoints in the cryptographic inventory, is possible. The simulation, however, is limited to small integers due to the current quantum hardware restrictions, but it is still functionally representative. Modern RSA security depends on the belief that classical methods cannot efficiently factor integers, but Shor's algorithm overturns this belief by giving the chance of polynomial-time factorization on very powerful quantum computers. As a result, the Shor simulation's outcomes support Quantum Sentinel's designation of the RSA and ECC installations as "quantum-fragile" primitives in the context of readiness scoring.

6. Conclusions

In this paper the authors suggested the Quantum Sentinel, an AI-based framework for quantum threat assessment and mitigation that is proactive. The framework automatically creates a cryptographic inventory using real-world CT evidence, identifies quantum-vulnerable deployments mainly consisting of RSA/ECC, and assesses enterprise readiness through the QPR under different adversary scenarios (NEAR, MID, and QDAY). The application of AI models for threat intelligence further increases the capacity by predicting and high accuracy and explainability ranking of the high-risk endpoints. Moreover, simulations of Shor and Grover based on Qiskit provide an executable validation of quantum attack feasibility which in turn strengthens the threat model's correctness. The paper concludes with the demonstration of PQC/hybrid mitigation planning which indicates the significant improvement of QPR through the simulated migration thereby providing actionable transition roadmaps.

In the future, the plan is to implement Quantum Sentinel in the actual enterprise networks, include full cryptographic telemetry beyond CT data, and validate the PQC migrations through real hybrid TLS experiments (OQS + OpenSSL). Other extensions will also comprise deep learning-based threat prediction, continuous monitoring pipelines, and the provision of adaptive crypto-agility mechanisms for the automated enforcement of PQC.

Declarations

Funding:

This research was supported by a grant (No. CRPG-25-3258) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

Author Contribution

S.M.A. conceived and designed the study. S.M.A. and M.K. contributed to data acquisition, analysis, and interpretation. S.M.A. drafted the initial manuscript. M.K. critically revised the manuscript for important intellectual content. Both authors reviewed and approved the final version of the manuscript.

Acknowledgement

This research is supported by a grant (No. CRPG-25-3258) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

Data Availability

The datasets used and/or analyzed during the current study available from the corresponding author on reasonable request.

References

1. Mohammed, A. Quantum-Resistant Cryptography: Developing Encryption Against Quantum Attacks. *J. Innovative Technol.*, 1(1). (2018).
2. Bishwas, A. K. & Sen, M. Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat. *arXiv preprint arXiv:2411.09995*. (2024).
3. Ganesh, R., Khan, B. U. I., Khan, A. R. & Kamsin, A. B. A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. *Int. J. Inf. Secur.* **24** (5), 1–45 (2025).
4. Wu, F., Zhou, B., Song, J. & Xie, L. Quantum-resistant blockchain and performance analysis. *J. Supercomputing.* **81** (3), 498 (2025).
5. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ...Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909), 237–243..
6. Joshi, A., Bhalgat, P., Chavan, P., Chaudhari, T. & Patil, S. Guarding against quantum threats: A survey of post-quantum cryptography standardization, techniques, and current implementations. In *International Conference on Applications and Techniques in Information Security* (pp. 33–46). Singapore: Springer Nature Singapore. (2024), November.
7. Scott, M. On TLS for the Internet of Things, in a Post Quantum world. *Cryptology ePrint Archive*. (2023).
8. Sjöberg, M. Post-quantum algorithms for digital signing in Public Key Infrastructures. (2017).
9. Sowa, J. et al. Post-quantum cryptography (pqc) network instrument: Measuring pqc adoption rates and identifying migration pathways. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (Vol. 1, pp. 1835–1846). IEEE. (2024), September.
10. Marchsreiter, D. Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems. *IET Blockchain.* **5** (1), e12094 (2025).
11. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ...Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909), 237–243..
12. Geremew, A. & Mohammad, A. Preparing critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically relevant quantum computing. *Int. J. Eng. Sci. Technol.* **6** (4), 338–365 (2024).
13. Jyothi Ahuja, N. & Dutt, S. Implications of quantum science on industry 4.0: Challenges and opportunities. *Quantum and blockchain for modern computing systems: vision and advancements: quantum and blockchain technologies: current trends and challenges*, 183–204. (2022).
14. Kuforiji, J. The importance of integrating security education into university curricula and professional certifications. *Int. J. Technol. Manage. Humanit.* **11** (03), 1–10 (2025).
15. Pandeya, G. R., Daim, T. U. & Marotzke, A. A strategy roadmap for post-quantum cryptography. In *Roadmapping Future: Technologies, Products and Services* (171–207). Cham: Springer International Publishing. (2021).
16. Marrow, A. A. *Quantum Computing: Evaluating the Threat Landscape and Risk Management Strategies* (Doctoral dissertation, Capitol Technology University). (2025).
17. Baseri, Y., Chouhan, V., Ghorbani, A. & Chow, A. Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. *Computers Secur.* **150**, 104272 (2025).
18. Yavuz, A. A., Nouma, S. E., Hoang, T., Earl, D. & Packard, S. Distributed cyber-infrastructure 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. (2022), December.
19. Khalil, K., Idriss, H., Idriss, T. & Bayoumi, M. Lightweight hardware security and physically unclonable functions. *Journal Hardw. Security* (2025).
20. Qader, T. *Systematic Security: Building Quantum Security: Preparing for Q-Day and Beyond* (CRC, 2026).
21. Pal, D. & Sau, D. Quantum Computing: Threat to Cybersecurity. In *Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategies* (161–188). Singapore: Springer Nature Singapore. (2025).
22. Sarkar, A. & Jhamb, M. A novel ultra-low power post quantum approach using artificial intelligence based key generation for cyber physical system in Internet of things. *Sustainable Computing: Inf. Systems*, 101242. (2025).
23. Rani, A., Ai, X., Gupta, A., Adhikari, R. S. & Malaney, R. Obfuscated quantum and post-quantum cryptography. *arXiv preprint arXiv:2508.07635*. (2025).
24. Saeed, M. M. An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption. *IEEE Access* (2025).
25. He, L. et al. A Post-Quantum Blockchain and Autonomous AI-Enabled Scheme for Secure Healthcare Information Exchange. *IEEE J. Biomedical Health Informatics* (2025).
26. Mujlid, H. M. & Alshahrani, R. Quantum-driven security evolution in IoT: AI-powered cryptography and anomaly detection. *J. Supercomputing.* **81** (9), 1–29 (2025).
27. Alkhatib, M. A Multifaceted Deepfake Prevention Framework Integrating Blockchain, Post-Quantum Cryptography, Hybrid Watermarking, Human Oversight, and Policy Governance. *Computers* **14** (11), 488 (2025).
28. Sharma, A. & Rani, S. Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices integrated With Deep Learning. *IEEE Trans. Consumer Electronics* (2025).

Figures

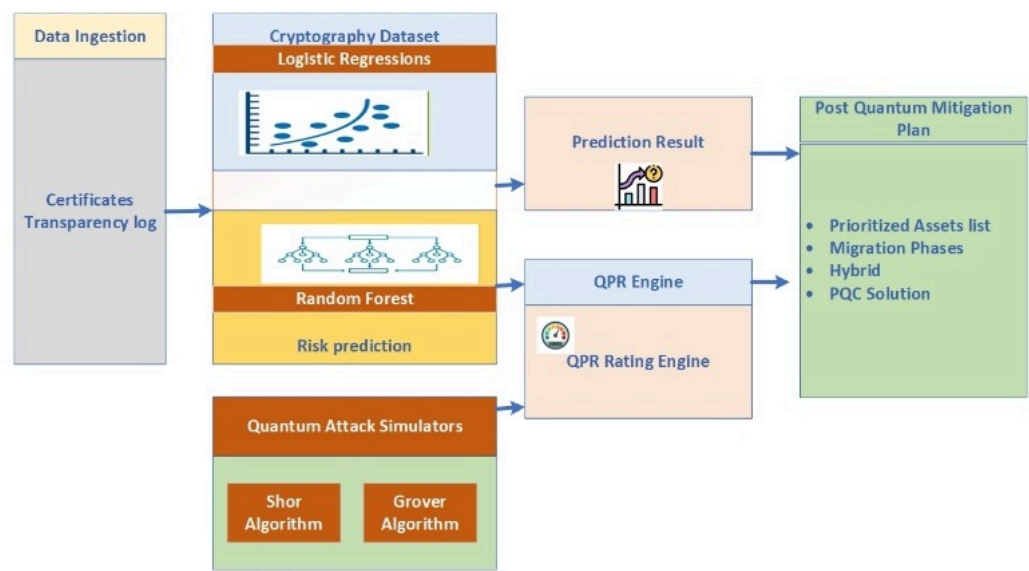


Figure 1
Quantum sentinel architecture flowchart.

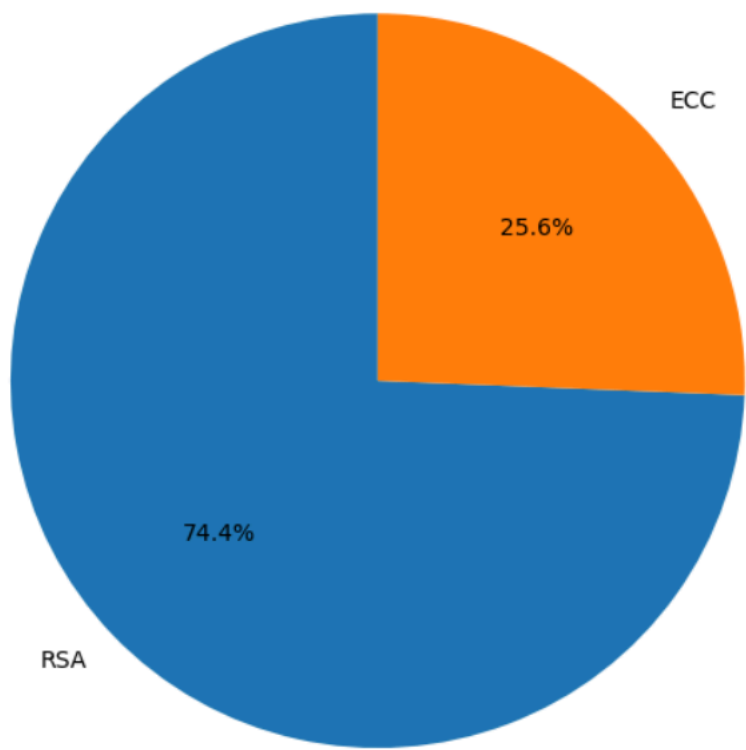


Figure 2
Algorithm Distribution – RSA vs ECC Bar Chart

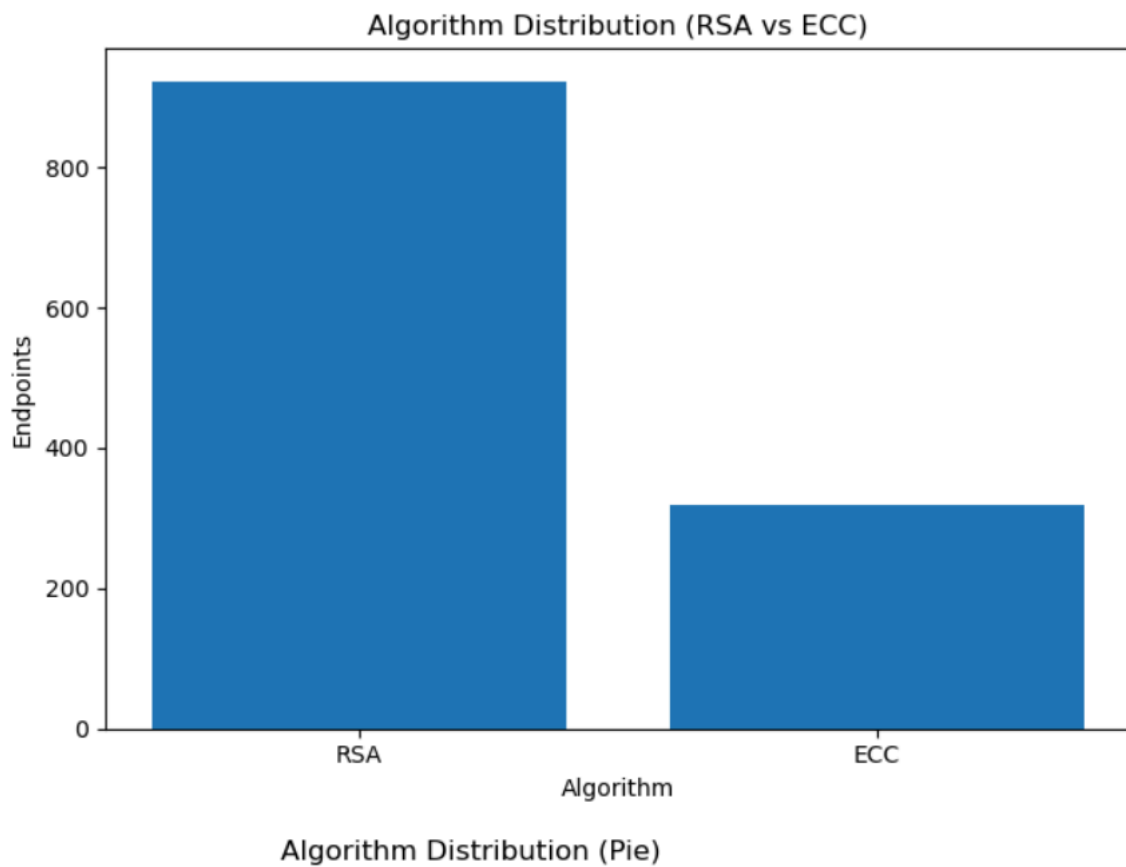


Figure 3

Algorithm Distribution – Pie Chart), RSA constitutes 74.4% of observed TLS endpoints.

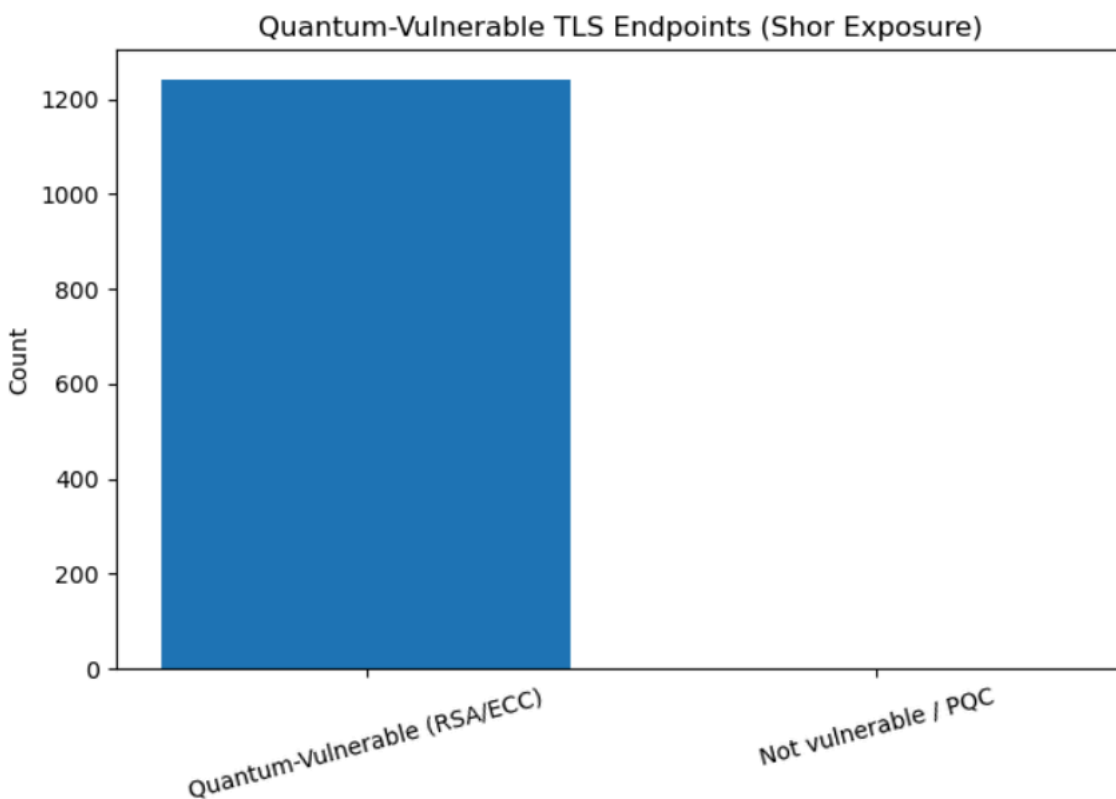


Figure 4

Quantum-Vulnerable TLS Endpoints / Shor Exposure

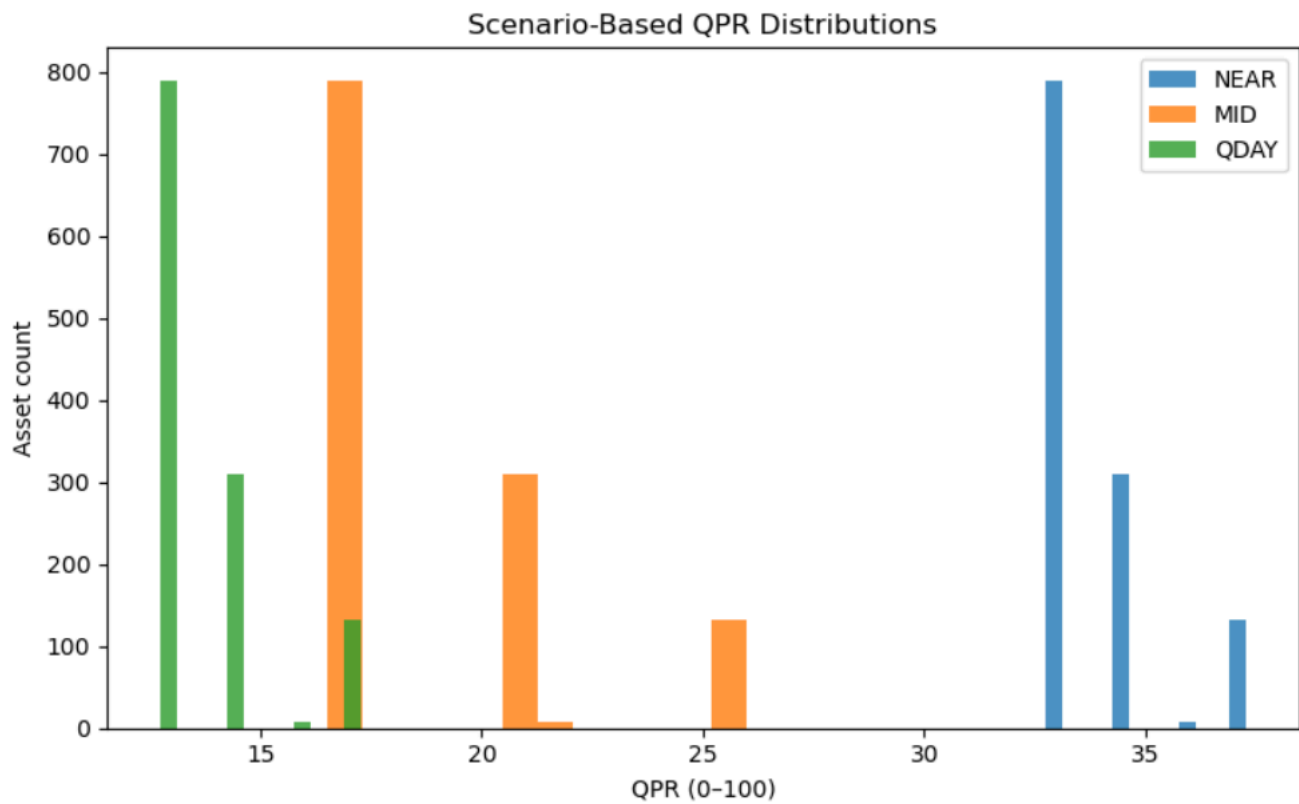


Figure 5

Scenario-Based QPR Distributions.

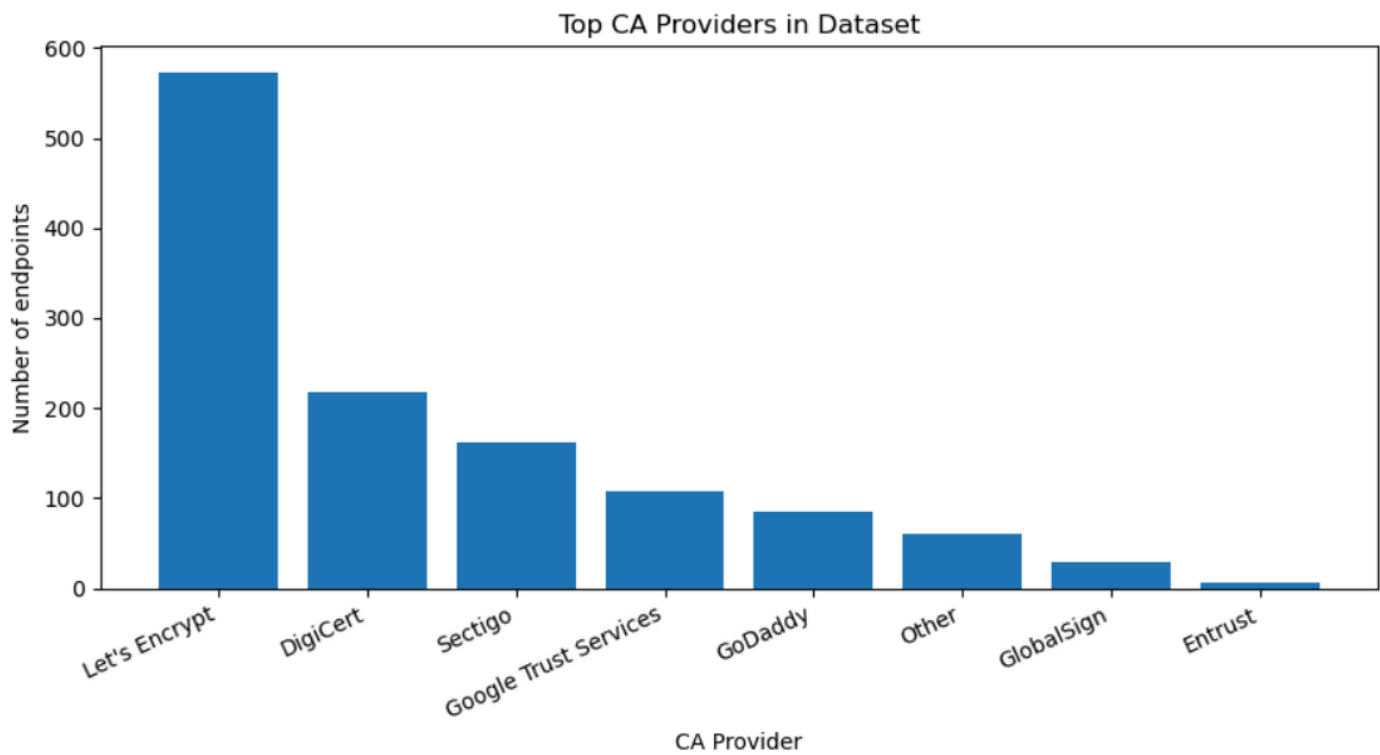


Figure 6

Top CA Providers in Dataset.

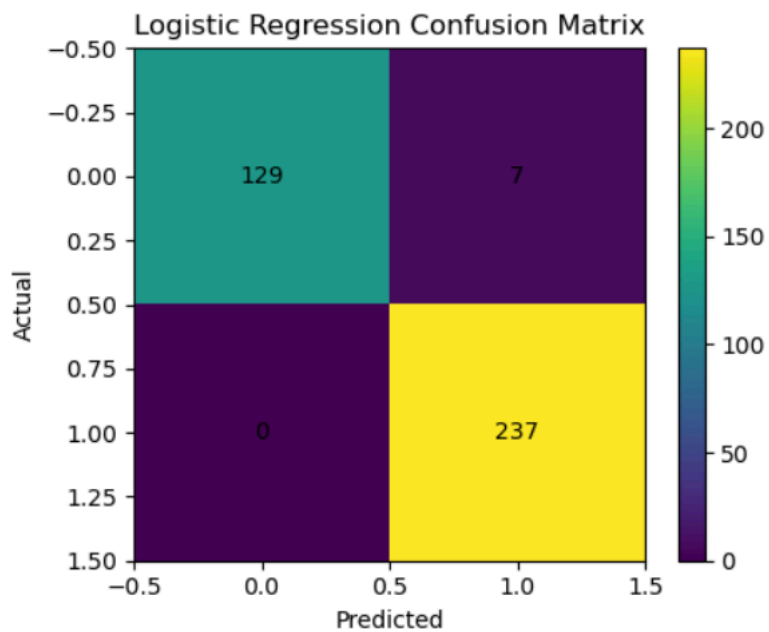


Figure 7

Logistic Regression Confusion Matrix.

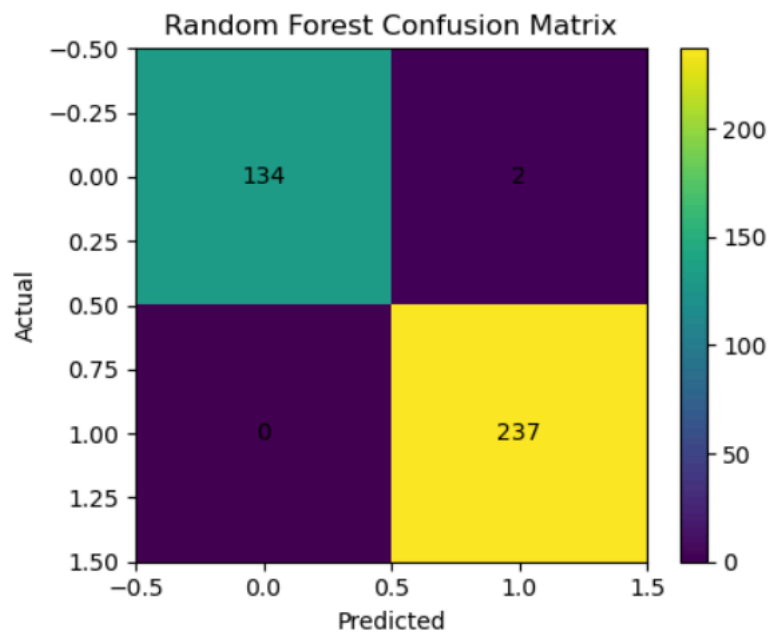


Figure 8

Random Forest confusion matrix.

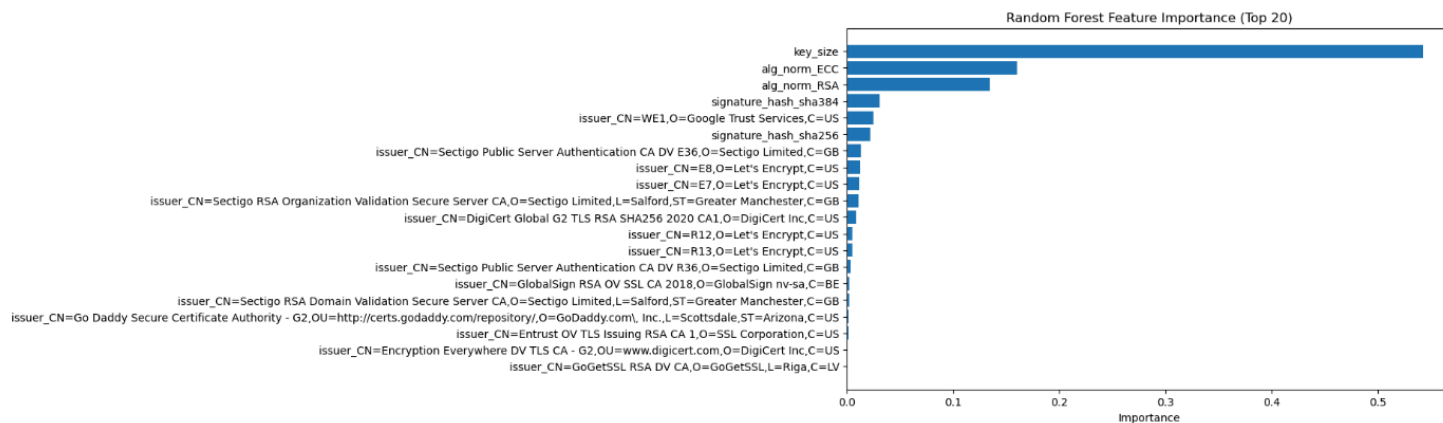


Figure 9

Feature Importance.

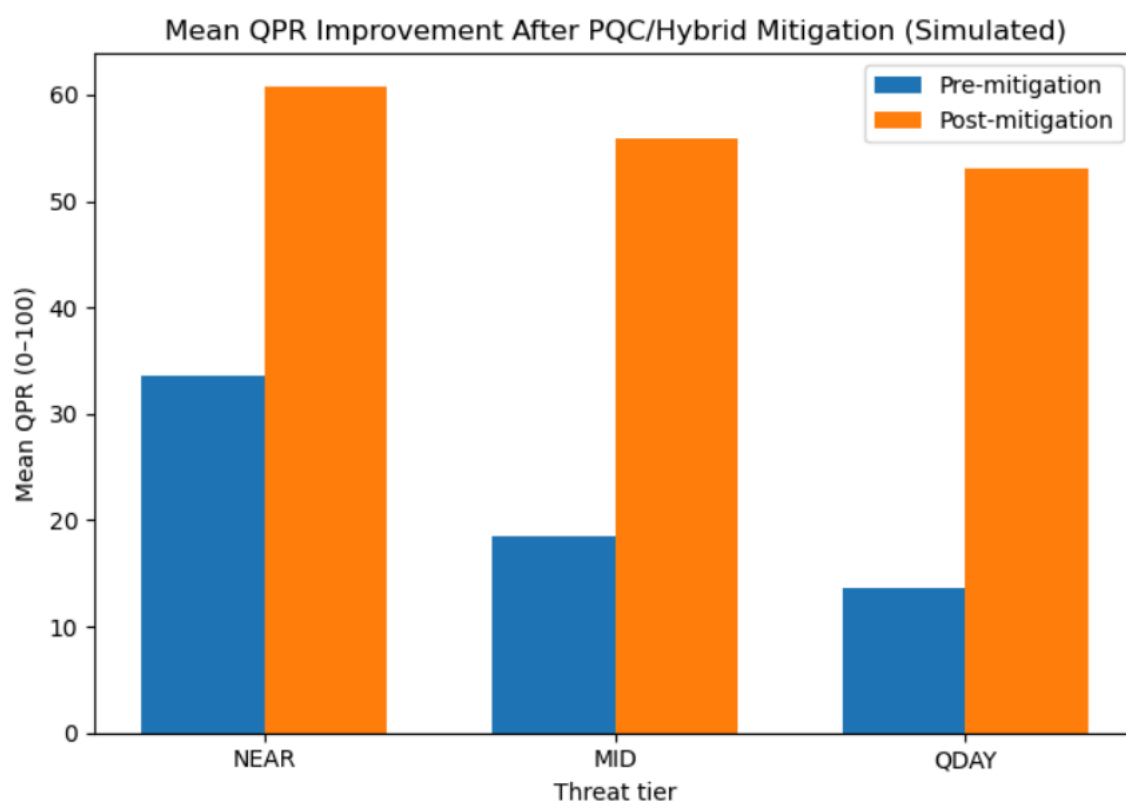


Figure 10

Mean QPR Improvement After PQC/Hybrid Mitigation.

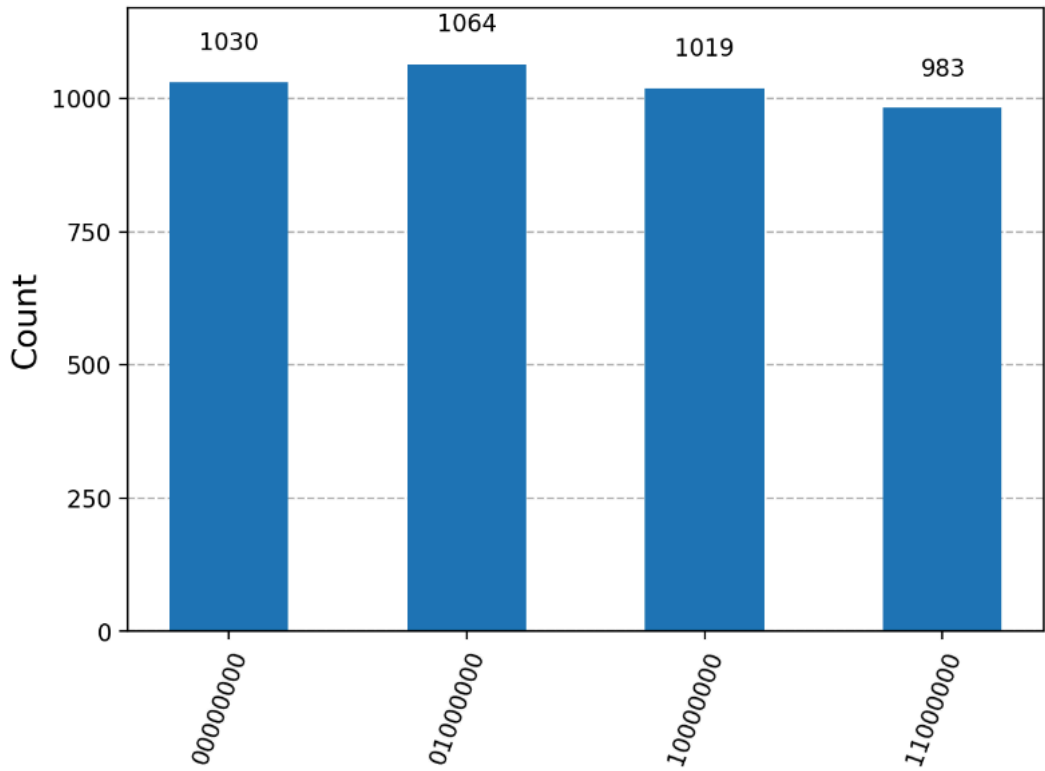


Figure 11

Shor Order-Finding PoC Measurement Distribution.