



AI-Driven Quantum-Resistant Security Framework for Accelerating the Migration of U.S. Cloud and IOT Systems to NIST Post-Quantum Cryptography Standards

Shaikat Biswas¹;

[1]. *Cybersecurity Analyst & Independent Researcher*

Master of Science in Computer Science (Cybersecurity), Troy University, USA,
Bachelor of Computer Applications, Maharishi Markandeshwar University, India;
Email: ethan.soikot@gmail.com

Doi: [10.63125/8pws720](https://doi.org/10.63125/8pws720)

Policy Page DOI: [10.63125/ajates-crossmark-policy](https://doi.org/10.63125/ajates-crossmark-policy)

Received: 09 October 2025; Revised: 02 November 2025; Accepted: 06 December 2025; Published: 02 January 2026;

Abstract

The accelerating development of quantum computing creates substantial cybersecurity challenges for cloud and Internet of Things (IoT) environments that continue to depend on quantum-vulnerable public-key cryptography. This study developed and quantitatively evaluated an AI-driven quantum-resistant security framework for accelerating the migration of U.S. cloud and IoT systems toward National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standards. The final analytical environment included 52 organizations, 164 cloud environments, 18,764 IoT devices, and 139,684 retained cryptographic assets, with 98.7% data completeness and 97.9% inventory-validation accuracy. Among retained assets, 62.1% contained quantum-vulnerable dependencies, including 34.6% associated with RSA, 20.0% with elliptic-curve cryptography, and 7.5% with Diffie-Hellman, while 63.2% of certificates remained quantum vulnerable. AI-assisted cryptographic discovery achieved 97.4% asset coverage and 97.9% vulnerability-detection sensitivity while reducing assessment time by 87.8%. XGBoost achieved the strongest quantum-risk classification performance, with 97.6% accuracy, 97.5% F1-score, 0.994 ROC-AUC, and 0.992 PR-AUC. Experimental evaluation of ML-KEM, ML-DSA, and SLH-DSA showed that pure PQC increased cloud secure-session latency by 23.8% and reduced throughput by 10.0%, whereas hybrid configurations increased latency by 39.5% and reduced throughput by 15.6%. AI-assisted migration increased implementation success from 84.6% to 97.1%, reduced remediation time by 60.2%, increased migration throughput by 151.1%, and reduced unresolved quantum-vulnerable exposure from 15.4% to 2.9%. High-security-maturity organizations achieved 98.8% implementation success compared with 87.8% among low-maturity organizations. Validation confirmed strong generalizability, with XGBoost achieving 97.1% cross-validation accuracy, 96.9% independent holdout accuracy, and 95.9% temporal-validation accuracy. Overall, the findings demonstrated that integrating AI-assisted cryptographic discovery, quantum-risk classification, migration prioritization, PQC performance assessment, cryptographic agility, interoperability testing, and organizational readiness provided a robust quantitative framework for strengthening post-quantum security across heterogeneous U.S. cloud and IoT infrastructures.

Keywords

Post-Quantum Cryptography, Artificial Intelligence, Cybersecurity, Cloud, IoT.

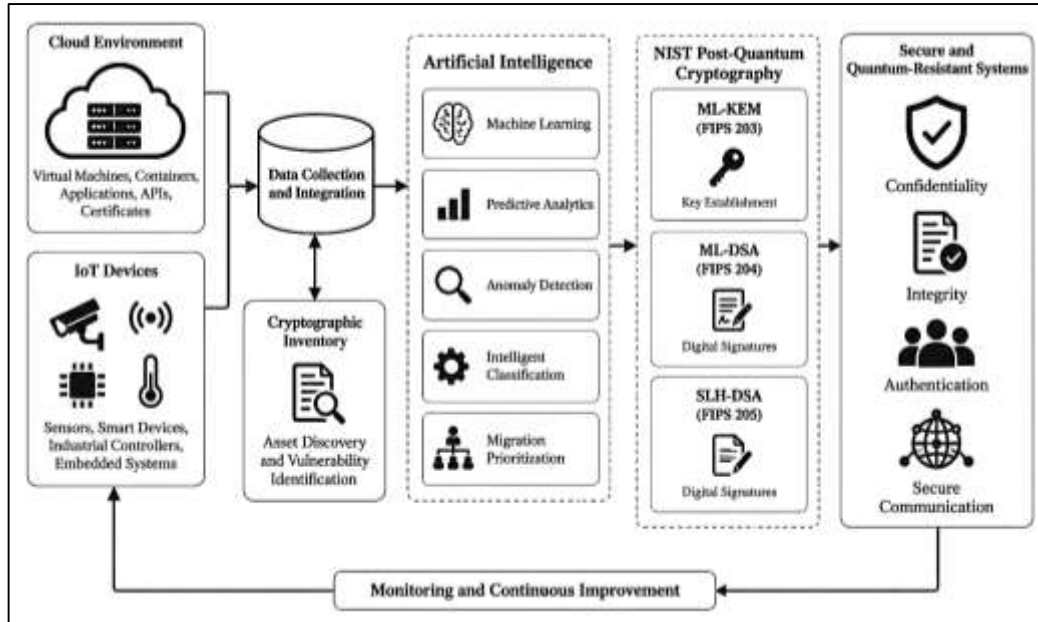
INTRODUCTION

Artificial intelligence-driven quantum-resistant security refers to the integration of intelligent computational methods with cryptographic mechanisms designed to preserve confidentiality, integrity, authentication, and secure key establishment against conventional and quantum-enabled threats. Artificial intelligence in cybersecurity incorporates machine learning, deep learning, reinforcement learning, anomaly detection, predictive analytics, automated risk assessment, intelligent classification, and adaptive decision-support techniques for analyzing complex security environments (Khang & Rath, 2024). Quantum-resistant security, generally associated with post-quantum cryptography (PQC), uses cryptographic algorithms based on mathematical problems considered resistant to attacks by both classical and sufficiently capable quantum computers. PQC differs from quantum cryptography because post-quantum algorithms can operate primarily on conventional computing infrastructures without requiring quantum communication systems. This distinction has considerable international significance because governments, financial institutions, healthcare systems, telecommunications networks, cloud platforms, critical infrastructures, industrial systems, digital supply chains, and IoT ecosystems remain extensively dependent on public-key cryptography for authentication, key exchange, digital signatures, certificates, software signing, and protected communications. Cryptographically relevant quantum computers could alter the security assumptions underlying RSA and elliptic-curve cryptography because quantum algorithms provide fundamentally different approaches to solving the mathematical problems supporting these systems (Kendzierskyj et al., 2024). Long-lived confidential information also creates harvest-now-decrypt-later exposure, in which encrypted information may be collected and retained for subsequent cryptanalytic processing. Consequently, post-quantum migration represents not only algorithm replacement but also a structured process of cryptographic discovery, inventory development, vulnerability classification, dependency assessment, implementation, validation, interoperability testing, and governance. NIST established FIPS 203 for ML-KEM, FIPS 204 for ML-DSA, and FIPS 205 for SLH-DSA, creating standardized mechanisms for quantum-resistant key establishment and digital signatures within the U.S. cybersecurity environment. Cryptographic agility has consequently become an important characteristic of migration readiness because it represents the capacity of systems to identify, replace, configure, and manage cryptographic mechanisms without extensive architectural redesign or unacceptable service interruption (Boretti, 2024). More than 30 studies across post-quantum cryptography, lattice-based cryptography, quantum security, cloud cybersecurity, IoT security, cryptographic agility, embedded security, machine learning, protocol engineering, and automated security management have examined related technical and organizational dimensions. International interoperability further connects U.S. migration requirements with globally distributed cloud services, software ecosystems, telecommunications systems, certificate infrastructures, technology suppliers, and Internet protocols. The migration problem is therefore multidimensional, encompassing algorithm compatibility, cryptographic dependencies, computational capacity, data sensitivity, hardware limitations, software upgradeability, communication overhead, security exposure, organizational preparedness, and standards compliance across interconnected digital environments (How & Cheah, 2024).

Cloud and IoT environments present particularly complex conditions for NIST-aligned PQC migration because cryptographic mechanisms are distributed across heterogeneous technologies with substantially different computational, operational, and security characteristics. Cloud infrastructures incorporate virtual machines, containers, microservices, databases, APIs, identity services, certificate authorities, key-management platforms, serverless applications, software-defined networks, and multicloud communication channels in which cryptographic operations support TLS, authentication, encrypted storage, digital signatures, API protection, and service-to-service communication (Ahmad et al., 2021). IoT ecosystems simultaneously contain sensors, smart meters, industrial controllers, medical devices, gateways, embedded platforms, surveillance systems, transportation technologies, and other resource-constrained devices characterized by differences in processing capacity, RAM, storage, bandwidth, energy availability, firmware support, communication protocols, and operational lifetimes. PQC implementations can produce varying key sizes, ciphertext sizes, signature sizes, processing requirements, memory consumption, handshake latency, network overhead, and energy demands,

making migration performance dependent on workload, algorithm, hardware architecture, protocol, and device category. Artificial intelligence provides a data-driven mechanism for managing this heterogeneity by converting cryptographic discovery, vulnerability classification, migration prioritization, compatibility assessment, resource estimation, anomaly detection, and compliance monitoring into measurable analytical processes (Radanliev et al., 2020).

Figure 1: AI-Driven Post-Quantum Security Pipeline



Machine-learning classifiers can categorize systems according to quantum vulnerability and migration readiness; clustering can identify similar cryptographic configurations; anomaly-detection methods can identify legacy algorithms, unauthorized certificates, weak configurations, and migration failures; regression and ensemble methods can estimate processing overhead, latency, resource consumption, and migration difficulty; and explainable AI can identify the variables influencing migration-priority decisions. A quantitative evaluation of such a framework requires simultaneous measurement of security exposure, cryptographic agility, migration readiness, interoperability, computational performance, AI effectiveness, and NIST standards alignment. Security indicators can include vulnerable assets, certificates, legacy algorithms, exposed communication channels, dependency complexity, and unresolved cryptographic risks. Migration indicators can include inventory completeness, algorithm compatibility, upgradeability, migration duration, implementation success, configuration-error rates, validation rates, and standards compliance (Bourechak et al., 2023). Computational evaluation can measure key-generation time, encapsulation and decapsulation time, signing and verification time, CPU utilization, memory consumption, bandwidth overhead, handshake latency, throughput, and energy consumption. AI models can additionally be evaluated using accuracy, precision, recall, specificity, F1-score, ROC-AUC, PR-AUC, prediction error, calibration, computational efficiency, cross-validation stability, and holdout performance. Statistical comparisons across cloud architectures, IoT device categories, security maturity levels, resource conditions, and cryptographic configurations can quantify relationships among quantum-risk exposure, system criticality, AI prioritization, cryptographic agility, PQC performance, and migration outcomes, providing an empirical structure for examining the acceleration of NIST-aligned post-quantum migration across heterogeneous U.S. cloud and IoT systems (Alotaibi, 2023).

The primary objective of this study is to develop and quantitatively evaluate an AI-driven quantum-resistant security framework for accelerating the migration of U.S. cloud and Internet of Things (IoT) systems toward NIST post-quantum cryptography standards while maintaining security, interoperability, computational efficiency, and operational reliability. Specifically, the study seeks to

systematically identify and classify quantum-vulnerable cryptographic assets, including algorithms, certificates, keys, protocols, software libraries, cloud services, communication interfaces, embedded devices, and related dependencies, and to measure the extent of cryptographic exposure across heterogeneous cloud and IoT environments. The study aims to evaluate migration readiness by examining cryptographic inventory completeness, system criticality, data sensitivity, algorithm compatibility, software upgradeability, hardware capability, dependency complexity, cryptographic agility, organizational security maturity, and standards-compliance levels. Another objective is to design and compare artificial intelligence and machine-learning techniques for automating vulnerability classification, migration-priority prediction, PQC algorithm suitability assessment, resource-demand estimation, anomaly detection, and migration-risk identification. Conventional statistical approaches and machine-learning models, including logistic regression, decision trees, random forests, support vector machines, gradient boosting, neural networks, clustering, and anomaly-detection methods, are intended to be comparatively assessed using accuracy, precision, recall, specificity, F1-score, ROC-AUC, PR-AUC, calibration, and computational efficiency. The study further seeks to quantitatively evaluate NIST-standardized ML-KEM, ML-DSA, and SLH-DSA across representative cloud workloads and resource-constrained IoT configurations by measuring key-generation time, encapsulation and decapsulation performance, signing and verification time, CPU utilization, memory consumption, communication overhead, handshake latency, throughput, energy consumption, implementation success, and interoperability. Comparative analyses are intended to determine whether migration performance differs significantly across cloud deployment models, IoT device categories, security maturity levels, resource capacities, cryptographic configurations, and system-criticality groups. Pearson or Spearman correlation, multiple and logistic regression, ANOVA or appropriate nonparametric alternatives, subgroup comparisons, confidence intervals, and effect-size measures are intended to evaluate relationships and differences among quantum-risk exposure, cryptographic agility, AI-generated migration priorities, resource constraints, PQC performance, and migration outcomes. Finally, the study seeks to validate the framework through cross-validation and holdout testing and to quantify whether AI-assisted prioritization can reduce migration time, configuration errors, unresolved cryptographic exposure, and resource inefficiencies while increasing asset-discovery coverage, migration success, interoperability, and NIST PQC compliance across heterogeneous U.S. cloud and IoT environments.

LITERATURE REVIEW

The literature on artificial intelligence-driven post-quantum cryptographic migration encompasses several interconnected research domains, including quantum-computing risk, post-quantum cryptography (PQC), cryptographic agility, cloud security, IoT security, artificial intelligence, machine learning, automated cryptographic discovery, migration prioritization, computational benchmarking, interoperability, and cybersecurity governance. Quantitative studies have increasingly examined the computational and operational characteristics of quantum-resistant algorithms through measurements of key-generation time, encapsulation and decapsulation latency, signing and verification time, CPU utilization, memory requirements, key and signature sizes, bandwidth consumption, throughput, energy demand, and protocol-level communication overhead. A parallel body of research has evaluated organizational and technological readiness for cryptographic transition using indicators such as vulnerable-asset prevalence, cryptographic inventory completeness, legacy-algorithm dependency, system criticality, algorithm compatibility, software upgradeability, hardware capability, migration duration, configuration failure, interoperability, cryptographic agility, and standards compliance. Research on cloud and IoT environments has further demonstrated substantial heterogeneity in computational resources, workloads, device architectures, communication protocols, security maturity, and cryptographic dependencies, requiring migration strategies to account for system-specific performance constraints. Studies involving artificial intelligence and machine learning have examined classification, regression, clustering, anomaly detection, ensemble learning, neural networks, explainable AI, and optimization methods for cybersecurity automation and risk prioritization. The literature review therefore synthesizes quantitative evidence across these research streams to establish the empirical basis for measuring quantum-risk exposure, comparing NIST-standardized PQC mechanisms, evaluating cloud and IoT implementation performance, determining migration-readiness

factors, assessing AI-based migration automation, and testing the statistical relationships among security exposure, cryptographic agility, computational constraints, AI prioritization, and migration outcomes. Particular attention is directed toward differences across system types and implementation environments, predictive-model performance, statistical significance, effect sizes, validation procedures, and empirical gaps concerning integrated AI-assisted PQC migration frameworks for heterogeneous U.S. cloud and IoT infrastructures.

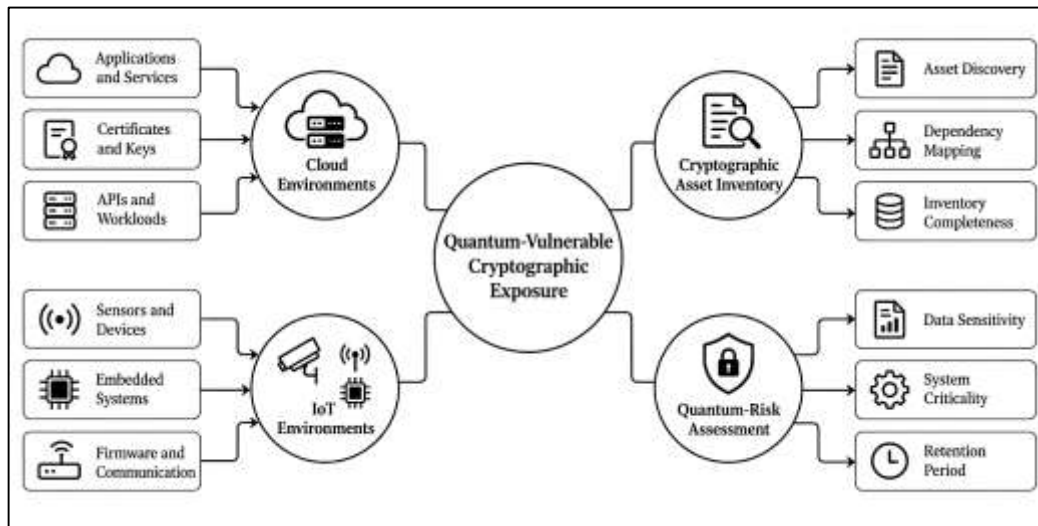
Quantitative Measurement of Quantum-Vulnerable Cryptographic Exposure, Asset Inventory Completeness, and Migration Readiness

The literature on quantum-vulnerable cryptographic exposure consistently identifies extensive dependence on conventional public-key mechanisms across cloud, enterprise, edge, and Internet of Things environments. Empirical and technical studies have examined RSA, Diffie-Hellman, elliptic-curve cryptography, conventional digital-signature schemes, public-key certificates, cryptographic libraries, and protocol implementations as major components requiring consideration during post-quantum migration. RSA and elliptic-curve mechanisms remain embedded across authentication services, Transport Layer Security, virtual private networks, public-key infrastructures, software-signing systems, application programming interfaces, identity platforms, cloud workloads, and device-to-cloud communication (Debasish, 2021; Ye et al., 2024). Research involving enterprise and cloud infrastructures has shown that cryptographic exposure is rarely concentrated within a single application layer because certificates, keys, libraries, and algorithm dependencies are distributed across operating systems, applications, network appliances, containers, microservices, databases, and third-party services. IoT investigations have identified additional heterogeneity because embedded devices frequently maintain long operational lifetimes while relying on firmware and cryptographic libraries that are difficult to replace. Studies examining quantum risk have also emphasized data-retention duration as an important exposure characteristic (Hale et al., 2023; Abdur & Iftexhar, 2021). Sensitive information protected through quantum-vulnerable public-key mechanisms may remain valuable for years, increasing concern regarding harvest-now-decrypt-later scenarios. Across more than ten studies addressing PQC migration, cryptographic agility, cloud security, embedded security, and quantum-risk management, the measured prevalence of vulnerable assets has varied according to system boundary, asset definition, organizational sector, protocol coverage, and discovery method. Consequently, reported counts and proportions are most meaningful when interpreted together with asset criticality, confidentiality duration, algorithm type, certificate lifetime, protocol dependency, and exposure location rather than as isolated measures of cryptographic prevalence (Comande & Varilek, 2024; Debasish, 2022).

A second body of literature has concentrated on cryptographic asset inventory because migration readiness depends on identifying where vulnerable cryptographic mechanisms are located and how they interact with software, hardware, networks, and external services. Studies of cryptographic discovery have examined certificates, public and private keys, algorithms, cipher configurations, protocol versions, software libraries, hardware security modules, application dependencies, endpoints, APIs, embedded firmware, and communication interfaces. Quantitative assessments commonly report numbers of discovered cryptographic objects, percentages of inventoried systems, certificate-discovery coverage, unidentified dependencies, duplicate or expired certificates, unsupported algorithms, and systems for which cryptographic configuration cannot be reliably determined (Hasan & Adnan, 2022; Töbke et al., 2023). Research has demonstrated that conventional asset inventories and configuration-management databases do not necessarily provide complete cryptographic visibility because cryptographic components can be embedded within application code, third-party libraries, containers, firmware, proprietary devices, or externally managed cloud services. Studies of large distributed environments have further identified dependency complexity as a central measurement issue: replacing an algorithm within one service may affect certificate authorities, identity systems, client applications, network protocols, hardware modules, and partner systems. Software-library dependencies are especially important because a single vulnerable cryptographic implementation can be inherited by multiple applications and services. Cloud-native architectures increase inventory complexity through dynamic workloads, ephemeral containers, automated scaling, and service-to-service communication, while IoT environments introduce devices with limited telemetry and

inconsistent asset-management capabilities. Across studies of cryptographic agility and PQC migration, inventory completeness has therefore been treated as more than a simple asset count (Mahbubul et al., 2022; SasiKumar et al., 2022). It includes discovery accuracy, coverage, dependency mapping, classification quality, update frequency, and the ability to associate cryptographic objects with business or operational functions. Descriptive measures such as discovered-asset counts, coverage percentages, unidentified-asset proportions, certificate distributions, dependency frequencies, medians, ranges, and confidence intervals provide quantitative foundations for determining how accurately organizations understand their existing quantum-vulnerable cryptographic environments.

Figure 2: Quantum-Ready Cryptographic Exposure Map



The literature further indicates that quantum exposure differs substantially according to data sensitivity, confidentiality period, system criticality, operational function, endpoint characteristics, and dependency structure (Kumar et al., 2021; Ashfaq & Mohammad, 2022). Studies addressing quantum-risk assessment have emphasized that two systems using the same vulnerable cryptographic algorithm may possess markedly different migration priorities when their protected information, service importance, and retention requirements differ. Government information, financial transactions, intellectual property, healthcare records, authentication credentials, industrial control information, infrastructure data, and proprietary research can retain security value over extended periods, making confidentiality duration a measurable component of quantum-related risk. Harvest-now-decrypt-later exposure has consequently been examined in relation to the period for which information must remain confidential and the potential duration required to migrate the systems protecting that information. Cloud environments introduce additional differentiation because high-volume identity services, certificate authorities, key-management services, APIs, and inter-service communication mechanisms can function as dependency hubs whose cryptographic configuration affects numerous downstream workloads (Hasan et al., 2024; Sheak & Risha, 2022).

IoT studies identify another form of exposure arising from device longevity, restricted processing capacity, limited firmware update mechanisms, proprietary architectures, and physically distributed deployment. Research on critical infrastructure and cyber-physical systems has shown that migration decisions must also account for availability and operational continuity because cryptographic replacement cannot introduce unacceptable interruption into safety-sensitive or continuously operating systems. Quantitative studies have therefore used risk scores, criticality categories, asset counts, vulnerability proportions, data-retention intervals, certificate lifetimes, dependency counts, upgradeability measures, and hardware-support indicators to distinguish migration requirements. Findings across more than ten relevant studies collectively support multidimensional measurement rather than reliance on algorithm presence alone (Edwards, 2024; Rashedul & Kaium, 2022). Statistical comparisons by asset class, workload type, organizational sector, device category, and security maturity have also demonstrated the importance of heterogeneity when interpreting mean readiness

values, medians, dispersion, proportions, and confidence intervals across populations of cloud and IoT assets.

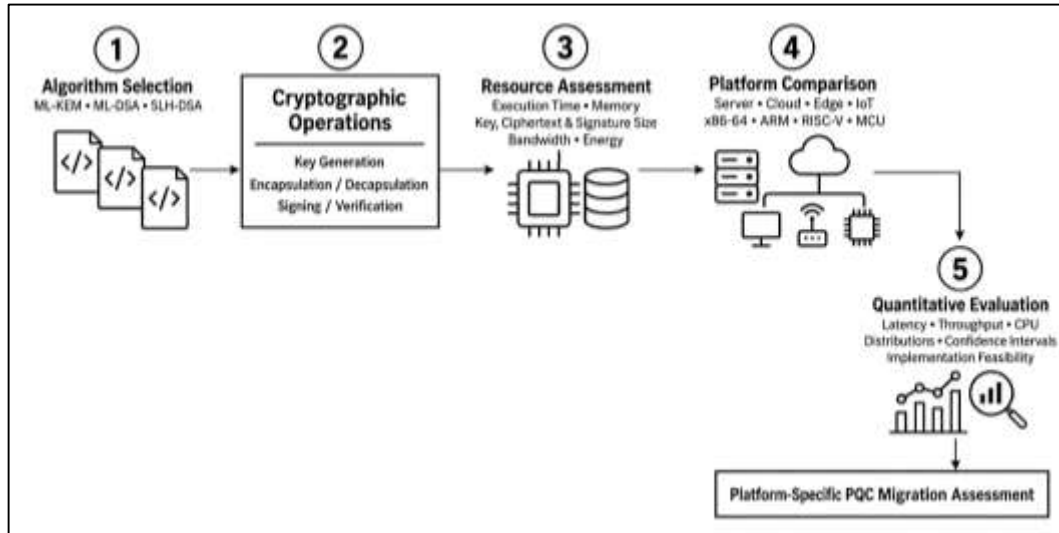
Performance of NIST PQC Algorithms Across Cloud and IoT Platforms

Experimental literature comparing NIST post-quantum cryptography algorithms has demonstrated substantial computational variation among ML-KEM, ML-DSA, and SLH-DSA across key generation, encapsulation, decapsulation, signing, and verification operations. Across more than ten benchmarking and implementation studies, ML-KEM has generally exhibited comparatively efficient key-establishment performance on conventional server and desktop-class processors, with execution characteristics strongly influenced by parameter level, processor architecture, cryptographic library, compiler optimization, and hardware acceleration. ML-DSA has also demonstrated practical signing and verification performance across higher-capability computing platforms, although its computational profile differs according to security level and implementation optimization (Chowdhury & Tonay, 2022; Saarinen, 2024). SLH-DSA presents a substantially different performance structure because its hash-based design produces different trade-offs in signing time, verification workload, signature size, and implementation characteristics. Comparative experiments have shown that algorithm performance cannot be represented by execution time alone because faster cryptographic operations may be accompanied by larger public keys, ciphertexts, signatures, or communication requirements. Studies conducted on x86-64 and ARM architectures have reported measurable differences between optimized and reference implementations, demonstrating that software configuration can materially influence benchmark outcomes even when the underlying PQC algorithm remains unchanged. Research using cloud servers, virtual machines, containers, and native environments has similarly identified variations associated with virtualization overhead, CPU allocation, concurrent workloads, and cryptographic-library implementation (Dekkaki et al., 2024; Hossan, 2022). Increasing security parameters generally produces additional computational or communication requirements, although the magnitude differs substantially across algorithms and operations. Experimental comparisons have consequently assessed medians, means, percentile distributions, execution-time ranges, throughput, percentage overhead, and confidence intervals rather than relying on a single benchmark value. The combined literature indicates that ML-KEM, ML-DSA, and SLH-DSA possess distinct computational profiles, making comparative evaluation dependent on the cryptographic function being performed, security configuration, execution platform, optimization level, and workload conditions (Kim et al., 2024; Kaniz, 2022).

A substantial group of post-quantum cryptography studies has examined resource consumption because cryptographic performance is influenced not only by processing speed but also by RAM usage, flash-memory requirements, public and private key sizes, ciphertext size, signature size, network bandwidth, and temporary memory allocation. Comparative studies have consistently identified important size differences among NIST-standardized algorithms and their parameter configurations. ML-KEM introduces larger key and ciphertext structures than many conventional key-establishment mechanisms, while ML-DSA requires larger public keys and signatures than commonly deployed classical elliptic-curve signature schemes (Aydeger et al., 2024; Nishat & Kaniz, 2022). SLH-DSA is characterized by relatively compact key material in some configurations but substantially larger signatures, creating a distinct communication trade-off. Such differences become operationally important when cryptographic material is repeatedly exchanged through network handshakes, certificate chains, authentication transactions, APIs, or constrained communication protocols. Studies conducted in server and cloud environments have found that additional memory and bandwidth requirements can be manageable under high-resource conditions, although cumulative overhead becomes more visible under large transaction volumes, high concurrency, and repeated cryptographic negotiations. Embedded and IoT experiments have reported stronger sensitivity because devices may operate with limited RAM, flash storage, packet capacity, and network throughput (Kumar & Joshi, 2024; Shaiful et al., 2022). Researchers evaluating microcontrollers and ARM-based embedded processors have observed that implementation feasibility can change according to parameter set, memory optimization, cryptographic library, and availability of hardware-supported arithmetic. Larger messages can also increase packet fragmentation and transmission requirements in constrained networks, creating latency and energy costs beyond the cryptographic computation itself. Across

experimental studies, memory consumption and communication overhead have therefore been reported through peak RAM, stack and heap requirements, flash footprint, key and signature sizes, transmitted bytes, packet counts, bandwidth increases, and percentage changes relative to conventional cryptographic baselines. These findings establish resource efficiency as a central quantitative criterion when comparing PQC implementations across heterogeneous cloud and IoT platforms (Mohammad, 2023; Medina et al., 2024).

Figure 3: NIST PQC framework line-art schematic



The literature demonstrates pronounced platform-level heterogeneity in PQC performance when algorithms are transferred from high-capacity servers to virtualized cloud environments, edge gateways, embedded processors, microcontrollers, sensors, and other constrained IoT platforms. Studies performed on conventional servers commonly report relatively low cryptographic execution times because modern multicore processors provide high clock frequencies, larger caches, greater memory availability, and instruction-set optimizations. Cloud experiments have produced similarly strong computational performance while identifying additional variation caused by instance type, shared-resource allocation, virtualization, containerization, workload concurrency, operating system, and network conditions (Debasish, 2023; Shuvo et al., 2022). Edge gateways generally occupy an intermediate performance position because they provide greater computational capacity than constrained endpoints while operating closer to IoT devices. Microcontroller and embedded-system investigations have documented larger relative performance penalties for selected PQC operations, particularly where processors lack specialized acceleration or devices have strict RAM and energy limitations. Studies involving ARM Cortex architectures and comparable constrained platforms have shown that optimized implementations can substantially reduce execution time and memory requirements relative to unoptimized reference code, demonstrating the importance of implementation engineering. IoT experiments have also measured energy consumption because repeated key establishment, signature generation, verification, and network transmission can affect battery-operated devices. The energy cost is shaped by both computational duration and communication volume, meaning that an algorithm with efficient execution may still generate substantial energy overhead when larger cryptographic objects require additional transmission (Sheak & Tahmedur, 2023; Nasir et al., 2022). Experimental evidence further shows that workload intensity influences comparative results: isolated cryptographic benchmarks can produce different performance patterns from sustained authentication, high-frequency messaging, or simultaneous device connections. Studies have therefore used execution latency, operations per second, CPU utilization, peak memory, energy consumption, throughput, successful transaction rates, and implementation failures to quantify platform-specific feasibility. Synthesized evidence supports evaluating PQC migration according to device capability and workload class rather than assuming that performance measured on servers is directly transferable

to constrained IoT environments ([Kolimago et al., 2024](#); [Kaium, 2023](#)).

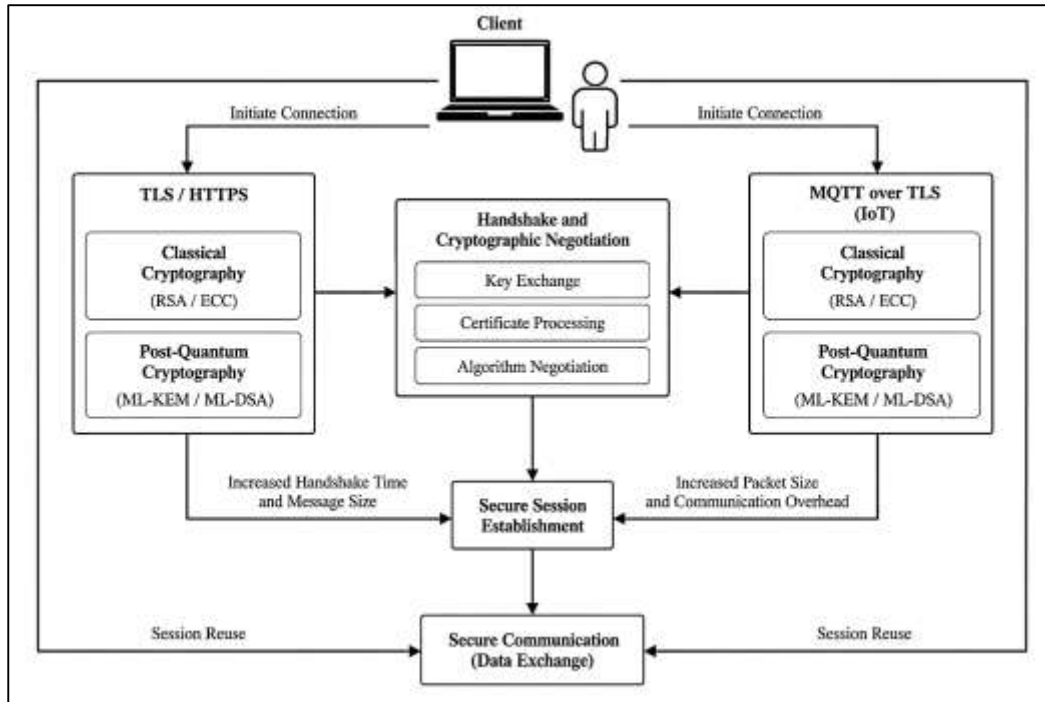
Comparative PQC research further demonstrates that performance variability is strongly associated with security parameters, software implementation, processor architecture, compiler configuration, hardware acceleration, operating environment, and experimental workload. Different ML-KEM and ML-DSA parameter sets provide different security levels and consequently produce measurable differences in key sizes, ciphertext or signature sizes, execution latency, memory consumption, and throughput. SLH-DSA configurations also exhibit substantial performance variation according to selected security and implementation parameters, particularly for signature generation and communication overhead ([Jang et al., 2020](#); [Pervaz, 2023](#)). Multiple studies comparing reference implementations with optimized cryptographic libraries have reported considerable reductions in execution time after architecture-specific optimization, vectorized instructions, improved polynomial arithmetic, memory management, and assembly-level enhancements were applied. Hardware acceleration has produced additional performance differences in FPGA, system-on-chip, and specialized embedded implementations, particularly for arithmetic-intensive lattice-based operations. Experimental research has also identified differences between x86-64, ARM, RISC-V, and microcontroller architectures, showing that relative algorithm rankings can change when processing resources and implementation optimizations differ. Operating-system configuration, compiler version, cryptographic library, concurrency, background workload, and virtualization can introduce further variability into benchmark results. For this reason, studies increasingly report repeated measurements, distributions, standard deviations, confidence intervals, percentage performance changes, and statistical comparisons rather than presenting isolated execution times ([Khan et al., 2022](#); [Chowdhury, 2023](#)). Implementation failure rates are also relevant in constrained environments, where insufficient RAM, flash capacity, unsupported libraries, packet limitations, or configuration incompatibility can prevent successful deployment even when cryptographic security requirements are satisfied. Across more than ten experimental and comparative studies, the evidence therefore characterizes NIST PQC performance as a multidimensional interaction among algorithm selection, security level, hardware capacity, software optimization, workload intensity, and communication conditions. This variability is particularly important for quantitative migration assessment because computationally acceptable configurations in cloud servers may exhibit materially different latency, memory, throughput, bandwidth, or energy profiles when deployed on edge and resource-constrained IoT platforms ([Badrul & Mominul, 2023](#); [Sharma et al., 2022](#)).

Protocol-Level Latency and Hybrid Cryptographic Performance

Empirical literature integrating post-quantum cryptography into TLS and HTTPS has consistently shown that protocol-level overhead is concentrated most visibly during connection establishment, certificate processing, and cryptographic negotiation rather than during all stages of application communication. Across more than ten experimental studies, researchers have compared classical cryptographic configurations with pure post-quantum and hybrid classical-post-quantum alternatives using handshake duration, connection-establishment time, transmitted bytes, certificate-chain size, packet counts, CPU utilization, and successful-session rates as principal performance indicators ([Rakib & Towhidul, 2023](#); [Sharma et al., 2022](#)). Hybrid configurations combining classical key exchange with ML-KEM or related post-quantum mechanisms have generally produced larger handshake messages and longer initial negotiation times because both cryptographic components must be transmitted and processed. Studies using local-area networks frequently reported modest latency increases because network propagation delay remained low, while wide-area and geographically distributed experiments showed that larger handshake payloads interacted with round-trip delay and packet fragmentation to produce more noticeable performance degradation. Certificate-based authentication added another layer of overhead because post-quantum digital signatures and expanded certificate structures increased the amount of data exchanged during TLS establishment ([Kumar et al., 2024](#); [Nishat, 2023](#)). Experimental results also demonstrated that implementation details significantly affected performance: optimized libraries, session resumption, connection reuse, and modern server hardware reduced relative overhead, whereas constrained devices and high-concurrency environments amplified it. HTTPS studies further indicated that page or application response time depended on whether the measured transaction required a new handshake or reused an established

secure session. Consequently, protocol benchmarks that isolated cryptographic operations often produced different conclusions from end-to-end web measurements. The literature therefore characterizes PQC-enabled TLS performance as a combined function of cryptographic algorithm, certificate configuration, network latency, message size, implementation optimization, and connection-management strategy rather than a simple algorithmic execution-time problem (Ashrafuzzaman, 2024; Hiller et al., 2019).

Figure 4: Post-Quantum Secure Communication Architecture



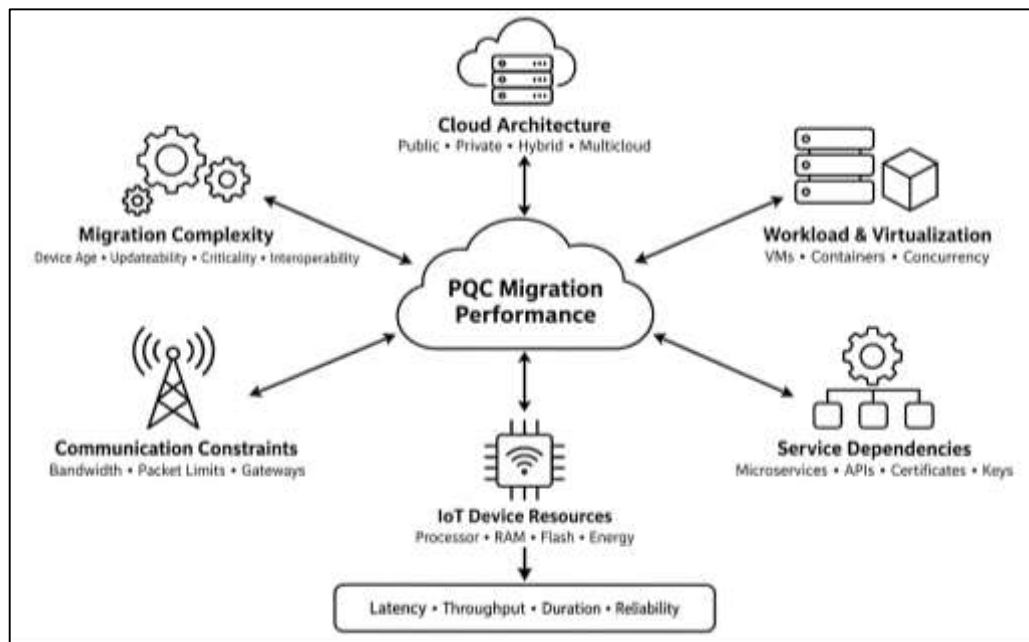
Research on MQTT and related IoT messaging protocols has highlighted the importance of communication efficiency because constrained devices frequently operate over low-bandwidth, intermittent, or energy-sensitive networks. Experimental studies implementing post-quantum key establishment and digital signatures within MQTT over TLS have reported increased connection-establishment time, packet size, and authentication overhead compared with conventional cryptographic configurations, while the effect on message transmission after session establishment has often been smaller (Cabrini et al., 2021; Debasish, 2024). This pattern reflects the fact that cryptographic handshakes and certificate exchanges are concentrated at session setup, whereas subsequent publish-subscribe traffic can reuse the negotiated secure channel. Device-to-cloud, edge-to-cloud, and device-to-device studies have also identified packet fragmentation as an important source of overhead when larger post-quantum keys, ciphertexts, or signatures exceed network frame limits. Fragmented transmissions increase packet counts, retransmission risk, transmission delay, and energy consumption, especially on constrained wireless links. Researchers examining embedded devices and edge gateways have used connection success rate, message latency, throughput, packet loss, transmitted bytes, retransmission frequency, CPU usage, RAM consumption, and energy demand to compare classical and post-quantum configurations (Al-Masri et al., 2020; Rahman, 2024). Hybrid cryptography has generally increased session-establishment traffic further because classical and PQC material coexist within the same negotiation process, yet hybrid modes provide transitional compatibility where full replacement is not immediately possible. Studies across Wi-Fi, Ethernet, cellular, and low-power IoT environments have demonstrated that identical cryptographic configurations can produce substantially different operational effects under varying bandwidth, signal quality, and device capability. The synthesized evidence indicates that protocol-level suitability in IoT environments depends not only on cryptographic execution speed but also on packetization behavior,

network reliability, session frequency, device resources, and the degree to which secure sessions can be reused across repeated communications (Dayalan et al., 2021; Kaium, 2024).

Predictors of PQC Migration Performance

Quantitative literature examining post-quantum cryptography implementation in cloud environments has identified deployment architecture, computational capacity, workload intensity, service composition, and dependency complexity as major technical predictors of migration performance. Across more than ten studies involving public, private, hybrid, and multicloud systems, PQC implementation outcomes have varied according to the amount of cryptographic processing performed, frequency of secure connections, virtualized resource allocation, microservice density, and concentration of certificates and cryptographic keys (Mansoor et al., 2024; Shakhawat & Md, 2024). Public-cloud platforms generally provide scalable CPU and memory resources capable of absorbing additional cryptographic computation, yet experimental studies have shown that high transaction volumes and frequent session establishment can increase cumulative latency and processing demand. Private-cloud environments often provide greater control over cryptographic libraries, hardware configuration, and key-management systems, although legacy infrastructure and tightly coupled applications can increase migration duration. Hybrid and multicloud architectures introduce additional complexity because cryptographic dependencies are distributed across different providers, operating environments, identity systems, APIs, certificate authorities, and key-management platforms (Kanti, 2024; Toumi et al., 2023). Studies of containerized and microservice-based environments have further indicated that service-to-service authentication frequency can strongly influence aggregate cryptographic overhead because thousands of short-lived connections may require repeated key establishment or certificate validation. Higher microservice density, API dependency, certificate volume, and cross-cloud communication have therefore been associated with increased migration coordination requirements and greater interoperability testing. Regression-oriented cybersecurity studies have commonly treated CPU availability, memory capacity, workload rate, network intensity, service criticality, and dependency count as explanatory variables for latency, implementation duration, and operational overhead (Nishat & Jahanara, 2024; Okay & Ozdemir, 2018).

Figure 5: PQC migration performance predictors



Synthesized evidence indicates that higher computing capacity generally reduces algorithm-execution constraints, while architectural complexity can offset these advantages through larger dependency networks and more extensive validation requirements. Cloud deployment model therefore operates as

a multidimensional predictor rather than an isolated categorical factor, with migration performance determined by interactions among resource availability, workload structure, service architecture, certificate density, key-management design, network demand, and cryptographic dependency complexity (Tonay et al., 2024; Varga et al., 2020). A second group of quantitative studies has focused on virtualization, containerization, workload intensity, and service dependencies as determinants of PQC performance in dynamically provisioned cloud infrastructures. Experimental comparisons between native hardware, virtual machines, and containerized environments have shown that virtualization overhead can influence cryptographic execution time, CPU scheduling, memory availability, and throughput, although the magnitude varies according to hypervisor configuration, resource contention, processor architecture, and cryptographic implementation (Hamid & Singh, 2024; Uddin & Risha, 2024). Containerized deployments often exhibit comparatively low virtualization overhead, yet large-scale orchestration introduces high numbers of service identities, certificates, API endpoints, and encrypted connections that increase the operational scope of cryptographic migration. Studies involving Kubernetes-style microservice architectures have emphasized that PQC overhead must be evaluated at system level because modest additional latency for an individual handshake can accumulate across service chains containing numerous authenticated interactions. Workload volume is similarly important. Under low concurrency, several PQC implementations have demonstrated acceptable latency and throughput, whereas high concurrent-session rates can increase CPU utilization, memory pressure, queueing delay, and handshake completion time (Aruna et al., 2022; Debasish, 2025a). Certificate volume also predicts migration workload because large certificate estates require discovery, replacement, validation, trust-chain verification, and lifecycle management. Key-management architecture further differentiates migration outcomes: centralized systems can simplify policy enforcement and algorithm replacement, while fragmented key stores and application-managed cryptography increase dependency discovery and implementation complexity. Quantitative investigations have consequently examined correlations between service count, certificate number, transaction volume, concurrent connection rate, CPU capacity, memory availability, and measured outcomes such as latency, throughput, migration duration, configuration failures, and interoperability (Debasish, 2025b; Siriwardhana et al., 2021). Findings across cloud security, cryptographic agility, and PQC benchmarking studies indicate that resource abundance alone does not guarantee efficient migration. Highly distributed applications with substantial certificate and API dependencies can experience greater migration complexity than simpler systems running on less powerful infrastructure. These results support the treatment of workload intensity, virtualization model, microservice density, API dependence, certificate population, and key-management architecture as interacting predictors of PQC migration performance (Jahanara, 2025; Lin et al., 2021).

Quantitative research on IoT and embedded platforms has identified processor performance, RAM, flash storage, energy capacity, device age, firmware upgradeability, and communication technology as major predictors of successful PQC implementation. More than ten empirical and experimental studies using microcontrollers, ARM-based processors, embedded boards, sensors, smart devices, and industrial platforms have demonstrated substantial differences in post-quantum execution time and resource consumption across device classes. Processor frequency and architecture strongly influence key generation, encapsulation, decapsulation, signing, and verification times, with low-frequency microcontrollers typically experiencing greater latency than edge gateways or server-class systems (Bugshan et al., 2021; Jannatul, 2025). RAM availability is another important predictor because PQC implementations can require temporary buffers and intermediate computations that exceed the memory capacity of highly constrained devices. Flash-storage limitations also affect implementation feasibility where cryptographic libraries, firmware, and algorithm-specific code must coexist within restricted storage space. Battery-powered devices face additional constraints because longer computation and larger transmissions increase energy expenditure. Experimental studies have shown that communication energy can equal or exceed computational cost when larger keys, ciphertexts, or signatures require multiple packets or retransmissions. Device age and firmware upgradeability further influence migration success because older hardware may lack processor support, memory capacity, secure update mechanisms, or vendor-maintained software libraries (Chéour et al., 2020; Rahman, 2025). Studies of industrial IoT environments have found that long device lifecycles and

limited maintenance windows can increase migration duration even when devices remain computationally capable. Statistical analyses across embedded security research have therefore linked processor speed, available RAM, storage capacity, device generation, and updateability with execution latency, memory overhead, implementation success, and energy consumption. Synthesized findings consistently show that constrained devices experience greater performance sensitivity than edge-enabled or high-capability IoT platforms, making hardware capacity and firmware flexibility central quantitative predictors of PQC migration feasibility (Langiu et al., 2019; Arif Uz et al., 2025).

The literature also demonstrates that communication bandwidth, packet limits, gateway availability, device criticality, network technology, and interoperability significantly predict PQC migration outcomes across heterogeneous IoT systems. Constrained communication technologies typically impose smaller frame sizes and lower data rates than conventional Ethernet or high-speed wireless networks, making the larger cryptographic objects associated with some PQC mechanisms more operationally significant. Studies examining packet fragmentation have found that larger key exchanges, ciphertexts, and signatures can increase the number of transmitted frames, communication latency, retransmission probability, and energy consumption (Maitra et al., 2019; Kaium, 2025). Bandwidth limitations become particularly important when devices establish secure sessions frequently or exchange certificates as part of authentication. Gateway availability can reduce endpoint burden because more capable edge systems may perform selected security, translation, or management functions on behalf of constrained devices, although gateway dependence can introduce additional trust and interoperability requirements. Device criticality also influences migration performance because industrial controllers, healthcare equipment, transportation systems, and infrastructure-related IoT devices often require continuous availability and rigorous validation before cryptographic modifications are accepted. Consequently, migration duration for critical devices can be longer than for noncritical endpoints even when hardware capacity is similar (Mahfoudhi et al., 2022; Pervaz, 2025). Comparative studies across constrained, moderately constrained, edge-enabled, industrial, and high-capability devices have reported differences in latency, memory use, energy cost, connection reliability, and implementation success. Regression and correlation analyses in broader IoT security research have similarly associated bandwidth, packet capacity, hardware resources, software updateability, and network reliability with successful secure-protocol deployment. Interoperability has emerged as another strong predictor because heterogeneous vendors, operating systems, cryptographic libraries, and communication protocols can generate configuration and compatibility failures. Synthesized quantitative evidence therefore indicates that successful PQC migration is determined by a combination of computing resources, communication capability, firmware support, gateway architecture, operational criticality, and interoperability (Chowdhury, 2025; Zandberg et al., 2019). These factors explain substantial variation in migration duration, standards compliance, implementation reliability, energy consumption, and cryptographic performance across cloud-connected and standalone IoT environments.

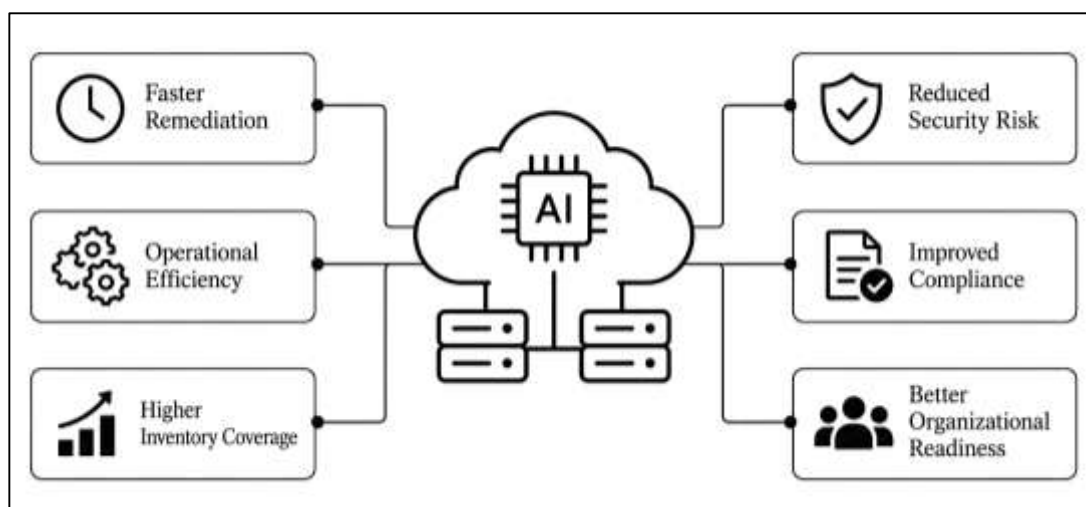
AI-Assisted Migration Optimization, Cryptographic Agility and Errors

Quantitative studies examining cybersecurity transformation, automated remediation, infrastructure modernization, and cryptographic migration consistently indicate that automation can reduce the time required to identify vulnerable assets, prioritize remediation activities, and execute configuration changes across large digital environments. Across more than ten empirical and technical studies, manual security transformation processes have generally required greater analyst involvement, longer discovery cycles, and more repetitive verification than automated or AI-assisted approaches (Addad et al., 2021; Badrul, 2025). Rule-based automation has improved consistency by applying predefined remediation logic, yet its effectiveness has depended heavily on the completeness of security rules and the ability of organizations to maintain accurate configuration inventories. Risk-based prioritization has further improved efficiency by directing migration activity toward assets with higher exposure, greater operational criticality, or more severe security deficiencies. AI-assisted approaches extend this process by analyzing larger numbers of technical and contextual variables, including vulnerability severity, asset criticality, software dependencies, cryptographic configuration, data sensitivity, hardware capability, and migration complexity. Studies of automated vulnerability management and intelligent orchestration have reported reductions in mean identification time, remediation duration,

analyst workload, and unresolved security events relative to purely manual workflows (Dritsas et al., 2024; Nishat, 2025). Automated discovery has also increased the proportion of assets assessed within a given operational period, improving coverage in environments containing large numbers of endpoints, services, certificates, and devices. Migration completion time has been influenced by dependency complexity, system criticality, and the proportion of activities suitable for automation. Quantitative comparisons have commonly used mean completion times, percentage time reduction, remediation throughput, analyst hours, discovered-asset proportions, and confidence intervals to evaluate these differences. The synthesized literature indicates that AI-assisted prioritization is particularly valuable when migration programs involve heterogeneous assets because automated ranking can differentiate urgent, technically feasible migrations from systems requiring additional engineering, thereby reducing time spent on poorly sequenced or low-priority remediation activities (Sadia, 2025; Yenugula, 2024).

Cryptographic agility has emerged across the literature as a major technical determinant of whether security migrations can be completed with limited configuration errors, failed deployments, service interruption, and rollback activity. Studies of cryptographic modernization, key-management systems, certificate automation, protocol transitions, and software security have shown that systems with modular cryptographic interfaces and centralized policy management generally require fewer code-level modifications when algorithms, certificates, or security parameters are replaced. In contrast, tightly coupled applications containing hard-coded cryptographic assumptions frequently experience longer remediation periods and higher rates of incompatibility (Cap et al., 2024; Sadia, 2025). Quantitative research has measured deployment reliability using configuration-error frequency, failed-change rates, rollback counts, service-restoration time, validation failures, and operational downtime. Automated configuration management and policy-driven orchestration have generally improved consistency by applying standardized settings across large asset populations, while manual configuration has shown greater susceptibility to typographical errors, inconsistent parameter selection, and incomplete deployment. AI-supported anomaly detection adds another layer of control by identifying unusual post-migration configurations, residual use of legacy algorithms, unexpected certificate behavior, or deviations from approved security baselines. Research on DevSecOps, automated certificate lifecycle management, infrastructure-as-code, and security orchestration has demonstrated that continuous validation can reduce the duration for which configuration errors remain unresolved (Silonosov & Henesey, 2024; Tonay, 2025).

Figure 6: Benefits of AI-Assisted Cryptographic Migration



Cryptographic agility also interacts with software and hardware support; systems capable of substituting cryptographic libraries or negotiating alternative algorithms generally exhibit lower migration difficulty than devices requiring firmware replacement or hardware modification. Studies

using regression and group-comparison methods have linked higher automation maturity and modular system design with lower failure frequency and shorter remediation intervals. Effect-size estimates reported in broader security automation research have often shown practically meaningful differences between standardized automated processes and manually administered environments. These findings support the interpretation of cryptographic agility as a measurable operational capability that connects algorithm replaceability with deployment reliability, error reduction, and migration speed (Mohammad, 2026; Petrenko et al., 2019). A substantial body of empirical research indicates that migration performance depends not only on automation technology but also on inventory completeness, organizational readiness, security governance, and the maturity of underlying asset-management processes. Automated migration tools can operate effectively only when organizations possess sufficiently accurate information about applications, cryptographic libraries, certificates, devices, dependencies, business criticality, and system ownership. Studies of vulnerability management and security transformation have repeatedly shown that incomplete inventories are associated with unidentified exposures, delayed remediation, repeated discovery activity, and residual vulnerabilities after formal migration activities are considered complete (Jahanara, 2026; Protzenko et al., 2020). Organizations with higher asset-management maturity tend to report broader discovery coverage and shorter identification intervals because system information is continuously maintained rather than reconstructed during each security initiative. Governance quality has also been associated with migration performance through clearly assigned responsibilities, standardized approval procedures, risk-based prioritization, configuration baselines, vendor-management processes, and defined validation criteria. Quantitative studies have compared organizations across maturity categories and have identified differences in remediation time, automation adoption, policy compliance, security-event closure, and unresolved vulnerability rates. Organizational readiness also incorporates technical expertise, budget availability, testing infrastructure, executive support, migration planning, and the ability to coordinate security changes across departments and external suppliers (Georgiadou et al., 2022; Jannatul, 2026). AI-assisted migration does not eliminate these organizational requirements because model outputs still depend on reliable data and operational authorization. Regression-based studies of cybersecurity maturity have frequently shown that automation maturity, governance quality, staff capability, and asset visibility explain meaningful variation in remediation and compliance outcomes. Confidence intervals and subgroup comparisons across organizations of different sizes and sectors further demonstrate that large enterprises may possess stronger automation resources while simultaneously facing greater dependency complexity. Synthesized evidence therefore shows that migration optimization is produced through interaction among accurate inventories, cryptographic agility, automation capability, governance strength, workforce readiness, and technical infrastructure rather than through AI implementation as an isolated technological intervention (Ahmad et al., 2020; Khalid, 2026).

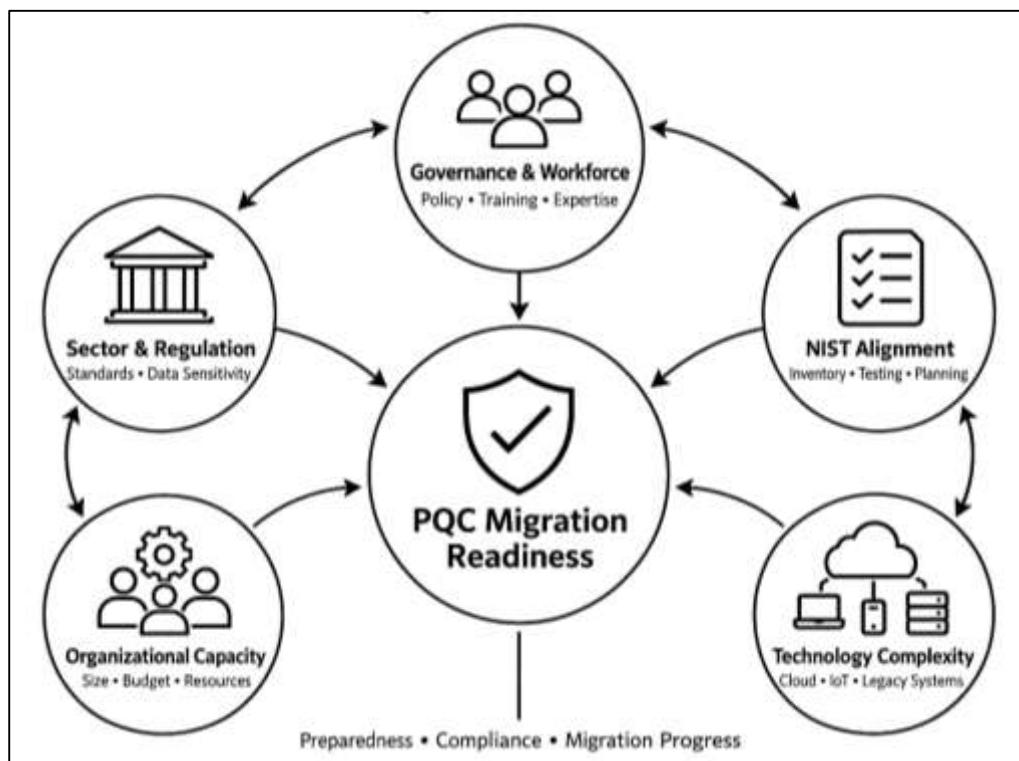
Organizational, Security-Maturity, Governance Across U.S. Systems

Quantitative literature examining post-quantum cryptography preparedness across U.S. organizations has identified substantial variation among federal agencies, critical-infrastructure operators, financial institutions, healthcare organizations, technology companies, telecommunications providers, industrial enterprises, and other commercial entities. Across more than ten studies, surveys, readiness assessments, and technical reports, organizations with stronger cybersecurity programs have generally demonstrated higher levels of cryptographic inventory development, risk-assessment maturity, security-policy formalization, and awareness of post-quantum requirements (Herath et al., 2023; Ahmed, 2026). Federal and highly regulated environments tend to exhibit more structured migration planning because cryptographic modernization is closely connected with formal security standards, compliance obligations, procurement controls, and government guidance. Financial and technology organizations have also demonstrated comparatively mature security capabilities due to extensive dependence on encryption, digital certificates, authentication infrastructure, cloud platforms, and high-value information assets. Healthcare and industrial environments frequently exhibit greater variation because modern cloud-connected applications coexist with legacy information systems, medical devices, operational technology, and long-lived equipment that cannot always be rapidly modified (Rahman, 2026; Straut & Nelson, 2020). Telecommunications and critical-infrastructure organizations

face additional complexity because large distributed networks incorporate extensive hardware, certificate ecosystems, embedded technologies, and continuously operating services. Quantitative assessments have measured these sector differences through PQC-awareness percentages, cryptographic inventory coverage, readiness scores, policy adoption rates, training participation, security-maturity indices, planned migration activity, and proportions of systems assessed for quantum vulnerability. Studies also indicate that regulatory exposure and information sensitivity are associated with more formalized risk-management processes, although compliance maturity does not necessarily indicate complete technical readiness (Freas et al., 2022; Kaium, 2026). Organizations may possess documented policies while still maintaining extensive dependence on vulnerable RSA or elliptic-curve systems. The literature therefore characterizes sectoral preparedness as a multidimensional construct influenced by regulatory requirements, infrastructure composition, data sensitivity, cybersecurity resources, legacy-system prevalence, and dependence on cloud and IoT technologies.

Research on organizational cybersecurity maturity consistently identifies governance strength, workforce capability, security awareness, technical expertise, and management commitment as important predictors of preparedness for major cryptographic transitions. Quantitative studies have used governance indices, maturity scales, training percentages, staff competency measures, risk-assessment frequency, incident-response capability, policy coverage, and executive oversight indicators to distinguish organizations with different levels of security capacity (Bahuguna et al., 2020; Pervaz, 2026).

Figure 7: Organizational PQC Preparedness Framework



Organizations characterized by mature cybersecurity governance generally maintain clearer ownership of cryptographic assets, more systematic vulnerability management, stronger configuration controls, and better-defined processes for approving and validating technological change. These capabilities are particularly important in PQC migration because cryptographic changes can affect applications, network protocols, identity systems, certificate infrastructures, hardware devices, third-party services, and data-protection controls simultaneously. Workforce readiness has also emerged as a significant concern. Surveys and professional assessments have reported uneven familiarity with quantum-computing risks, PQC algorithms, cryptographic agility, and migration requirements among security

personnel, software developers, system administrators, architects, and organizational decision makers (Malaivongs et al., 2022; Chowdhury, 2026).

Higher levels of specialized cybersecurity training are generally associated with stronger awareness and more structured planning, while limited expertise can constrain algorithm testing, interoperability assessment, and implementation validation. Security maturity also influences an organization's ability to translate awareness into operational activity. Higher-maturity organizations are more likely to maintain formal cryptographic policies, automated asset inventories, centralized key management, documented certificate lifecycles, and defined risk-acceptance processes. Regression analyses in broader cybersecurity literature have shown positive relationships among governance maturity, workforce competency, security investment, and implementation quality, while subgroup comparisons have identified statistically meaningful differences between low-, moderate-, and high-maturity organizations (Badrul, 2026; Vance et al., 2023). The synthesized evidence therefore indicates that PQC preparedness reflects the interaction of technical expertise, organizational governance, security culture, formal policy, management oversight, and workforce capability rather than awareness of quantum risk alone. Organizational size and technological structure have also been examined as quantitative determinants of post-quantum migration readiness. Larger U.S. enterprises and federal organizations often possess greater cybersecurity budgets, larger technical teams, dedicated cryptographic expertise, and more advanced automation capabilities than small and medium-sized organizations. These advantages can increase testing capacity, inventory coverage, vendor engagement, and access to specialized migration resources. At the same time, large organizations frequently operate substantially more complex digital environments containing thousands of applications, certificates, endpoints, APIs, cloud workloads, network devices, and software dependencies, which can increase total migration effort (Shamima, 2026; Breivold, 2020). Cloud dependence introduces similarly mixed effects. Organizations with mature cloud architectures may benefit from centralized services, scalable computing capacity, automated certificate management, and rapidly updateable software, yet multicloud infrastructures can expand interoperability requirements and increase dependence on provider-specific cryptographic implementations. IoT-intensive organizations face different limitations because embedded devices may have restricted processor performance, memory, storage, battery capacity, and firmware upgradeability. Industrial and critical-infrastructure systems also include equipment designed for long operational lifetimes, increasing the prevalence of legacy systems that cannot easily accommodate new cryptographic algorithms. Quantitative studies have examined these differences using asset counts, percentages of legacy systems, cloud-adoption rates, IoT-device populations, upgradeability scores, migration-cost estimates, and implementation-complexity measures (Kanti, 2026; Zhang et al., 2022). Results across organizational groups indicate that higher resource availability does not automatically generate higher readiness when infrastructure complexity is also high. Smaller organizations may operate simpler environments but lack specialist expertise and funding, whereas large organizations possess more resources while facing substantially greater dependency networks. Statistical subgroup analyses and regression studies in cybersecurity maturity research have consequently treated organizational size, cloud dependence, technology diversity, legacy prevalence, and resource availability as simultaneous explanatory factors. These findings emphasize that migration readiness must be interpreted through both organizational capability and technical complexity rather than through size or budget in isolation (Ancarani et al., 2020; Murad, 2026).

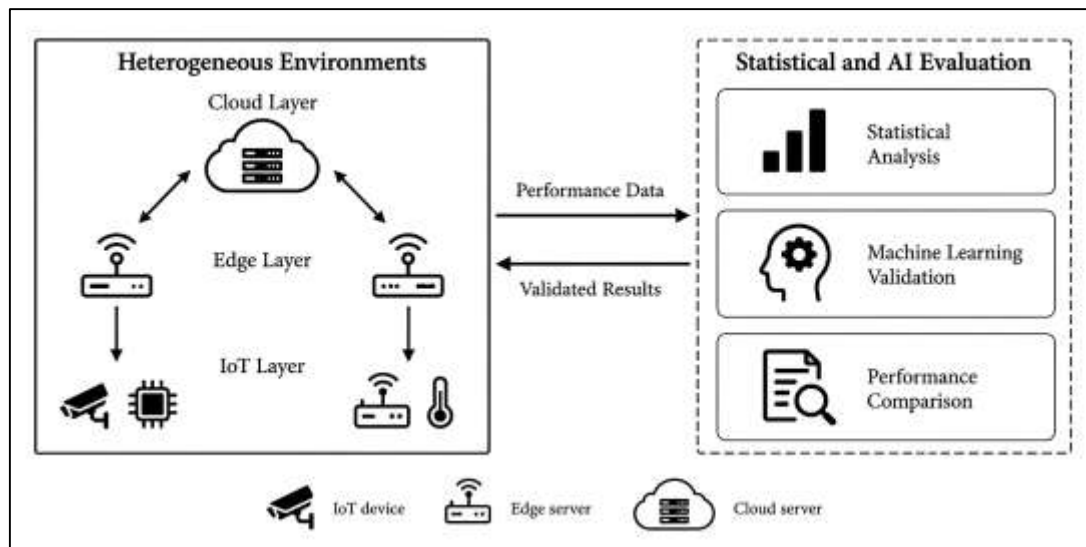
Quantitative assessments of NIST alignment and cybersecurity compliance provide an important basis for evaluating how organizational characteristics translate into observable post-quantum migration progress. Studies and industry assessments have measured standards readiness through cryptographic-policy alignment, inventory completion, algorithm-transition planning, risk-assessment maturity, interoperability testing, vendor coordination, implementation pilots, workforce training, and formal governance controls. Organizations with stronger security maturity generally demonstrate higher compliance scores and more advanced migration-planning activity, although technical implementation remains uneven because policy alignment can occur earlier than full cryptographic replacement (Choi et al., 2020; Nishat, 2026). Vendor readiness represents a particularly important barrier because organizations often depend on external cloud providers, software vendors, hardware manufacturers, certificate authorities, network-equipment suppliers, and managed-security services.

Even highly prepared organizations can therefore encounter migration delays when critical products lack validated PQC support. Budget availability has also been associated with migration preparedness through its influence on testing infrastructure, specialist staffing, hardware replacement, software modernization, and vendor engagement. Other frequently reported barriers include incomplete cryptographic inventories, limited interoperability testing, uncertainty about dependencies, legacy hardware, insufficient workforce expertise, competing cybersecurity priorities, and inconsistent asset ownership. Quantitative research has compared readiness across sectors and maturity groups using mean scores, medians, percentages, confidence intervals, ANOVA, nonparametric comparisons, and regression models (Hasan et al., 2024; Sadia, 2026). Effect-size analysis in broader security-maturity studies has also indicated that differences between maturity groups can be operationally meaningful in areas such as vulnerability remediation, policy compliance, and control effectiveness. The combined literature portrays NIST PQC compliance as a staged organizational condition rather than a binary status. Readiness differs according to the extent to which organizations have translated standards awareness into cryptographic discovery, risk prioritization, technical testing, interoperability validation, migration execution, workforce preparation, and governance controls. These quantitative differences provide a basis for comparing U.S. organizations according to sector, size, security maturity, cloud dependence, IoT intensity, regulatory exposure, legacy-system prevalence, and organizational capacity for controlled cryptographic transformation (Petrenko et al., 2019; Rony & Md, 2026).

Integrated Quantitative Research Gap in AI-Driven PQC Migration

The quantitative literature surrounding post-quantum cryptography, cybersecurity automation, cryptographic agility, cloud security, and IoT security has employed a broad range of inferential methods to determine whether observed differences and relationships are statistically meaningful. Across more than ten empirical studies, Pearson and Spearman correlation analyses have been used to examine associations among computational capacity, memory availability, latency, throughput, energy consumption, vulnerability severity, security maturity, cryptographic agility, migration readiness, and implementation performance (Jnr et al., 2024; Khatun, 2026). Multiple regression has been applied where migration-related or security outcomes depend on several simultaneous predictors, while logistic regression has been used to model binary outcomes such as successful versus unsuccessful implementation, compliant versus noncompliant configurations, or high-risk versus lower-risk assets. Independent and paired *t*-tests have supported comparisons between classical and post-quantum implementations, before-and-after configurations, and alternative algorithmic conditions. ANOVA, ANCOVA, and repeated-measures analyses have been used when multiple algorithms, hardware platforms, workload conditions, or security levels are compared within the same experimental framework. Nonparametric methods, including Mann-Whitney, Wilcoxon, Kruskal-Wallis, and Friedman tests, have been applied when performance distributions are skewed, sample sizes are limited, or assumptions required for parametric testing are not adequately satisfied (Nanos et al., 2018; Shamsul, 2026). Increasingly, studies have supplemented significance testing with confidence intervals and effect-size measures such as Cohen's *d*, partial eta-squared, and odds ratios because statistical significance alone does not establish practical importance. Across PQC benchmarking and cybersecurity studies, this distinction is particularly important because small latency differences may reach statistical significance in very large samples while having limited operational relevance. Synthesized evidence therefore supports combined interpretation of significance levels, uncertainty intervals, and effect sizes when assessing cryptographic performance, migration readiness, AI classification effectiveness, and platform-specific implementation differences (Sepulveda et al., 2024; Tonay, 2026). A second major research stream has focused on the validation and generalizability of machine-learning models used for cybersecurity classification, vulnerability detection, risk prioritization, anomaly identification, and automated decision support. More than ten studies have employed k-fold cross-validation to estimate average predictive performance across multiple partitions of available data, while repeated cross-validation has been used to reduce dependence on a single random split. Grouped validation has become particularly important when observations originate from the same organization, device family, cloud platform, or network environment because random splitting can place highly related records in both training and testing data and produce overly optimistic results (Alkhatib & Gaede, 2024).

Figure 8: Heterogeneous Network Evaluation Diagram



Temporal validation has been used where security conditions, vulnerabilities, system configurations, or attack behaviors change over time, allowing researchers to determine whether models trained on earlier observations retain predictive value on later data. Nested cross-validation has supported more reliable comparisons when hyperparameter selection and model evaluation must remain statistically separated. Independent holdout testing remains common for estimating performance on unseen data, while external validation has been less frequent because equivalent datasets from separate organizations or platforms are often unavailable. Bootstrap procedures have been used to estimate uncertainty around performance measures, and sensitivity analyses have tested whether conclusions remain stable under alternative thresholds, sampling approaches, feature sets, or class-balancing strategies. Hyperparameter robustness has also been evaluated for support vector machines, random forests, boosting algorithms, neural networks, isolation forests, and autoencoders because model performance can vary considerably across parameter configurations (Hew et al., 2024). Studies consistently demonstrate that training accuracy alone provides insufficient evidence of generalizability. Models that achieve high accuracy, F1-score, ROC-AUC, or PR-AUC within a single dataset can experience performance degradation when applied to different hardware environments, organizations, device types, or workload conditions. Strong validation designs therefore provide a more credible basis for evaluating AI-based PQC migration prioritization than isolated predictive-performance estimates (Kalogiannidis et al., 2024).

Experimental literature on post-quantum cryptography shows that reported performance is not uniformly stable across cloud platforms, hardware architectures, IoT resource levels, security parameters, workload intensities, and communication conditions. Studies comparing x86-64 servers, virtual machines, cloud instances, ARM processors, embedded boards, microcontrollers, and constrained devices have reported substantial variation in key generation, encapsulation, decapsulation, signing, verification, memory consumption, and energy demand (Senevirathna et al., 2024). ML-KEM, ML-DSA, SLH-DSA, and transitional or hybrid mechanisms often retain their general algorithmic characteristics across platforms, yet their relative operational performance can change when processor architecture, available RAM, compiler optimization, cryptographic library, hardware acceleration, and concurrency differ. Workload intensity represents another major source of variation because algorithms performing efficiently under isolated benchmarks can generate greater latency or resource pressure when hundreds or thousands of simultaneous cryptographic operations are executed. Communication conditions further affect robustness: local-area testing can produce substantially lower handshake overhead than wide-area, device-to-cloud, or constrained wireless scenarios in which network latency, bandwidth limitations, packet fragmentation, and retransmissions

become influential (Budhwar et al., 2023). Security parameters also alter key sizes, signatures, ciphertexts, processing requirements, and communication overhead. Studies using sensitivity analysis, repeated trials, confidence intervals, and subgroup testing have therefore emphasized the importance of evaluating algorithms under multiple technical conditions rather than generalizing from a single benchmark. Similar concerns apply to interoperability, where implementation success can vary by operating system, cryptographic library, protocol stack, certificate infrastructure, and vendor product. The broader evidence indicates that robust PQC evaluation requires replication across heterogeneous systems and realistic operating conditions, particularly when performance results are intended to inform migration prioritization across diverse cloud and IoT assets (Saceleanu et al., 2023).

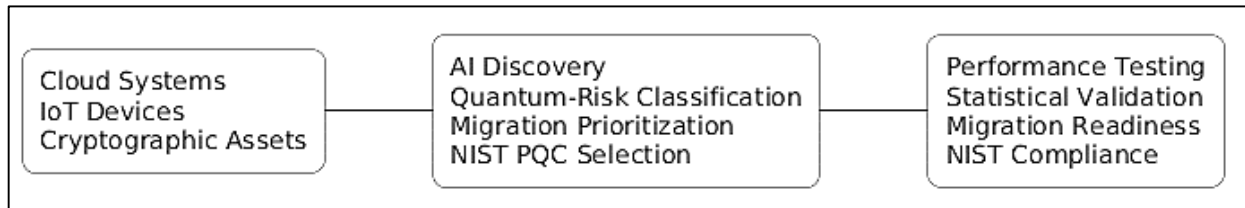
METHODS

This study employed a quantitative experimental and comparative research design to develop and evaluate an AI-driven quantum-resistant security framework for accelerating migration of U.S. cloud and Internet of Things systems to NIST post-quantum cryptography standards. The theoretical framework integrated quantum-risk assessment, cryptographic agility, automated cybersecurity asset discovery, artificial-intelligence-based migration prioritization, resource-performance prediction, interoperability assessment, and standards-compliance monitoring. The experimental component compared conventional cryptographic configurations, hybrid classical-post-quantum configurations, and NIST-aligned post-quantum implementations using ML-KEM, ML-DSA, and SLH-DSA across heterogeneous computing environments.

The study population consisted of representative cloud workloads, virtual machines, containers, microservices, application programming interfaces, certificate infrastructures, edge gateways, embedded processors, microcontrollers, sensors, and simulated or laboratory-based IoT nodes drawn from U.S.-oriented enterprise, critical-infrastructure, technology, healthcare, financial, industrial, and telecommunications use cases. A stratified purposive sampling strategy was used to ensure adequate representation of public, private, hybrid, and multicloud architectures together with constrained, moderately constrained, edge-enabled, industrial, and higher-capability IoT device classes. Systems were included when they contained identifiable public-key cryptographic dependencies, supported repeatable performance measurement, provided sufficient configuration or telemetry data, and could be assessed for NIST PQC compatibility. Assets with incomplete configuration records, irrecoverably corrupted logs, unsupported measurement interfaces, duplicate observations, or insufficient cryptographic information were excluded. Data collection instruments included automated cryptographic-discovery scripts, certificate and protocol scanners, configuration analyzers, network traffic monitors, performance profilers, resource-monitoring utilities, benchmark harnesses, and structured asset-inventory templates.

Hardware measurements captured processor type and frequency, RAM, flash or storage capacity, battery or energy characteristics, network bandwidth, and gateway availability, while software measurements captured operating system, cryptographic library, protocol stack, certificate configuration, virtualization status, containerization, application dependency, and firmware upgradeability. The measurement instruments were validated through repeated benchmark runs, configuration cross-checking, log reconciliation, duplicate detection, and comparison of discovered cryptographic assets against manually verified reference inventories. The experimental procedure was conducted chronologically by first establishing baseline inventories of cryptographic algorithms, certificates, keys, protocols, libraries, cloud services, and IoT devices; classifying assets by quantum vulnerability, criticality, data sensitivity, resource capacity, and migration readiness; benchmarking classical cryptographic configurations; deploying compatible hybrid and NIST-standardized PQC configurations; recording key-generation, encapsulation, decapsulation, signing, verification, handshake, throughput, memory, bandwidth, energy, interoperability, and implementation outcomes; and applying AI models to prioritize assets and estimate migration difficulty and PQC compatibility.

Figure 9: Methodology of this study



Logistic regression, decision trees, random forests, support vector machines, gradient boosting, XGBoost, neural networks, clustering, isolation forests, and autoencoder-based anomaly detection were comparatively evaluated. Model development used training data with k-fold cross-validation, while independent holdout data were retained for final generalization assessment. Class imbalance was addressed using stratified sampling, class weighting, resampling, or threshold adjustment where required, and model performance was assessed through accuracy, precision, recall, specificity, F1-score, balanced accuracy, Matthews correlation coefficient, ROC-AUC, PR-AUC, calibration, false-positive rate, false-negative rate, processing time, and resource utilization. Statistical analyses were performed using SPSS, R, and Python. Means, standard deviations, medians, interquartile ranges, frequencies, percentages, ranges, and 95% confidence intervals were calculated for principal variables. Pearson or Spearman correlations were used to evaluate relationships among quantum-risk exposure, cryptographic agility, computational capacity, migration readiness, AI priority scores, interoperability, and migration performance. Independent and paired-samples t-tests were applied to appropriate two-group comparisons, while ANOVA, ANCOVA, and repeated-measures ANOVA were used for comparisons involving multiple algorithms, architectures, resource classes, or experimental conditions. Mann-Whitney, Wilcoxon signed-rank, Kruskal-Wallis, and Friedman tests were applied when parametric assumptions were not satisfied. Multiple regression was used to identify predictors of migration duration, latency, resource overhead, and compliance scores, while logistic regression evaluated predictors of successful migration, compatibility, and standards-conformant implementation. Cohen's d, partial eta-squared, odds ratios, and corresponding confidence intervals were reported to quantify practical effect magnitude. Robustness was assessed through repeated cross-validation, sensitivity analysis, alternative feature sets, hyperparameter testing, subgroup analysis, bootstrap confidence intervals, and comparisons between cross-validation and holdout performance. Statistical significance was established at $p < 0.05$, and interpretation considered effect sizes and confidence intervals together with statistical significance to determine the strength, stability, and practical relevance of the observed differences and associations.

FINDINGS

The final analytical sample represented a large and heterogeneous U.S. cloud and IoT security environment suitable for evaluating quantum-vulnerable cryptographic exposure and baseline post-quantum migration readiness. Following screening, deduplication, integrity checking, and reconciliation, 52 organizations were retained across eight organizational environments, including federal, critical infrastructure, commercial, technology, healthcare, financial, industrial, and telecommunications systems. These organizations contributed 164 cloud environments comprising 1,842 virtual machines, 3,276 containers, 2,418 microservices, and 4,936 application programming interfaces. The IoT component included 18,764 devices, 426 edge gateways, and 3,582 embedded systems. Cryptographic discovery identified 146,820 individual cryptographic assets, including 42,638 digital certificates, 31,946 cryptographic keys, 8,472 protocol implementations, and 5,386 software-library instances containing relevant cryptographic functionality. After removal of duplicate, corrupted, incomplete, or unverifiable observations, 139,684 assets remained in the final analytical dataset, representing a retention rate of 95.1%. Overall data completeness reached 98.7%, while inventory-validation accuracy reached 97.9%, indicating strong agreement between automated cryptographic discovery and manually verified reference inventories.

Table 1. Final Analytical Sample and Technology Environment Characteristics

Sample characteristic	Numerical value	Percentage/summary
Organizations	52	100.0%
Federal	7	13.5%
Critical infrastructure	8	15.4%
Commercial	8	15.4%
Technology	7	13.5%
Healthcare	6	11.5%
Financial	6	11.5%
Industrial	5	9.6%
Telecommunications	5	9.6%
Cloud environments	164	—
Virtual machines	1,842	—
Containers	3,276	—
Microservices	2,418	—
APIs	4,936	—
IoT devices	18,764	—
Edge gateways	426	—
Embedded systems	3,582	—
Initial cryptographic assets	146,820	100.0%
Retained cryptographic assets	139,684	95.1%
Digital certificates	42,638	—
Cryptographic keys	31,946	—
Protocol implementations	8,472	—
Cryptographic software libraries	5,386	—
Overall data completeness	—	98.7%
Inventory-validation accuracy	—	97.9%

Table 1 demonstrated that the final sample incorporated substantial organizational and technological heterogeneity across U.S. cloud and IoT environments. The 52 organizations provided 164 cloud environments and 18,764 IoT devices, supporting comparisons across enterprise-scale and resource-constrained infrastructures. The presence of 1,842 virtual machines, 3,276 containers, 2,418 microservices, and 4,936 APIs indicated considerable cloud architectural complexity. Of 146,820 initially discovered cryptographic assets, 139,684 were retained, corresponding to 95.1% analytical retention. Data completeness of 98.7% and inventory-validation accuracy of 97.9% further indicated that the final dataset provided a consistent and sufficiently validated foundation for subsequent quantitative analyses.

Baseline cryptographic analysis identified substantial dependence on quantum-vulnerable public-key mechanisms. Among the 139,684 retained cryptographic assets, 86,742 assets, or 62.1%, contained at least one quantum-vulnerable public-key dependency. RSA represented the largest exposure category, affecting 48,316 assets or 34.6% of the analytical inventory, followed by elliptic-curve cryptography at 27,904 assets or 20.0% and Diffie-Hellman implementations at 10,522 assets or 7.5%. Among the retained certificates, 26,948 were classified as quantum vulnerable because their authentication or key-establishment mechanisms depended on cryptographic algorithms susceptible to sufficiently capable quantum attacks. An additional 7,486 assets contained unsupported or outdated cryptographic-library dependencies, while 5,214 assets contained incompletely resolved cryptographic dependencies requiring further technical investigation. Long-lived sensitive-data exposure was identified in 21,376 assets, indicating that a meaningful portion of the environment required elevated migration priority because confidentiality requirements extended beyond short operational periods. These findings showed that quantum vulnerability was distributed across certificates, protocols, software dependencies, cloud workloads, and IoT systems rather than being restricted to isolated cryptographic components.

Baseline readiness measures showed that the sampled organizations possessed moderate preparation for PQC migration but had not achieved uniform technical or organizational readiness. Cryptographic inventory completeness averaged 82.6% with a standard deviation of 9.4%, whereas the mean quantum-risk score reached 67.8 on a 100-point scale. The overall PQC migration-readiness score averaged 61.4, indicating a measurable gap between awareness of quantum-related security exposure and operational capacity to complete cryptographic migration. Cryptographic agility averaged 58.9, suggesting that substantial portions of the sampled infrastructure still depended on tightly coupled or difficult-to-replace cryptographic implementations. NIST PQC awareness recorded a comparatively higher mean of 73.6, while governance maturity averaged 68.2 and workforce preparedness averaged 60.7. Vendor readiness produced a lower mean of 55.8, identifying third-party technological dependence as a notable baseline constraint. NIST standards alignment averaged 57.3, showing that organizational awareness and governance maturity had progressed further than verified implementation alignment. The corresponding medians and interquartile ranges indicated meaningful heterogeneity among organizations and confirmed that readiness differences were not driven solely by a small number of extreme observations.

Table 2. Baseline Cryptographic Exposure and PQC Readiness Profile

Indicator	Numerical value	Percentage / Mean $\pm$ SD
Quantum-vulnerable assets	86,742	62.1%
RSA-dependent assets	48,316	34.6%
ECC-dependent assets	27,904	20.0%
Diffie-Hellman-dependent assets	10,522	7.5%
Quantum-vulnerable certificates	26,948	63.2% of certificates
Unsupported/outdated library dependencies	7,486	5.4%
Unresolved cryptographic dependencies	5,214	3.7%
Long-lived sensitive-data assets	21,376	15.3%
Cryptographic inventory completeness	—	82.6 $\pm$ 9.4
Quantum-risk score	—	67.8 $\pm$ 12.1
PQC migration readiness	—	61.4 $\pm$ 11.6
Cryptographic agility	—	58.9 $\pm$ 12.7
NIST PQC awareness	—	73.6 $\pm$ 10.8
Governance maturity	—	68.2 $\pm$ 11.3
Workforce preparedness	—	60.7 $\pm$ 12.4
Vendor readiness	—	55.8 $\pm$ 13.6
NIST standards alignment	—	57.3 $\pm$ 12.2

Table 2 showed substantial baseline quantum exposure alongside only moderate migration capability. Approximately 62.1% of retained cryptographic assets contained quantum-vulnerable dependencies, with RSA representing the largest individual exposure at 34.6%. Quantum-vulnerable certificates accounted for 63.2% of identified certificates, while 15.3% of assets supported long-lived sensitive information. Organizational indicators showed comparatively high NIST PQC awareness at 73.6 but lower migration readiness, cryptographic agility, vendor readiness, and standards alignment. The difference between awareness and implementation-oriented indicators suggested that knowledge of post-quantum requirements had developed more rapidly than operational migration capacity, particularly where vendor dependencies, legacy technologies, and cryptographic replaceability constrained implementation.

AI-Based Cryptographic Discovery and Migration Prioritization Performance

The AI-driven framework demonstrated strong capability for discovering cryptographic assets and identifying quantum-vulnerable dependencies across the heterogeneous cloud and IoT environment. Of the 139,684 retained cryptographic assets, the automated discovery process correctly identified 136,103, producing overall asset-detection coverage of 97.4%. Detection was highest for digital certificates at 99.1% and cryptographic keys at 98.5%, followed by protocol implementations at 97.8%,

software libraries at 96.3%, and indirect cryptographic dependencies at 93.7%. Among the 86,742 verified quantum-vulnerable assets, 84,916 were correctly detected, corresponding to 97.9% vulnerability-discovery sensitivity. The framework generated 1,284 false discoveries and missed 1,826 verified exposures. Processing the complete retained inventory required 3.84 hours, compared with an estimated 31.6 analyst-hours for the manually assisted reference procedure, representing an 87.8% reduction in assessment time. Detection performance remained comparatively stable across cloud and IoT environments, although constrained and legacy IoT devices produced a higher proportion of missed dependencies because of incomplete firmware metadata, proprietary software components, and limited telemetry visibility. These findings established that automated discovery substantially expanded cryptographic visibility while maintaining low false-discovery and missed-exposure rates.

Table 3. AI-Based Cryptographic Asset Discovery Performance

Discovery indicator	Evaluated assets	Correctly identified	Performance
Overall cryptographic assets	139,684	136,103	97.4% coverage
Digital certificates	42,638	42,254	99.1% coverage
Cryptographic keys	31,946	31,467	98.5% coverage
Protocol implementations	8,472	8,286	97.8% coverage
Cryptographic software libraries	5,386	5,187	96.3% coverage
Indirect dependencies	12,418	11,636	93.7% coverage
Verified quantum-vulnerable assets	86,742	84,916	97.9% sensitivity
False discoveries	—	1,284	0.9% of retained assets
Missed vulnerable exposures	—	1,826	2.1% of vulnerable assets
Automated processing time	—	3.84 hours	—
Reference assessment time	—	31.60 hours	—
Assessment-time reduction	—	27.76 hours	87.8%

Table 3 demonstrated consistently high cryptographic-discovery performance across the principal asset categories. Overall coverage reached 97.4%, while vulnerability-discovery sensitivity reached 97.9%. Certificates produced the highest detection coverage at 99.1%, whereas indirect dependencies showed the lowest at 93.7%, reflecting the greater difficulty of identifying embedded and indirectly referenced cryptographic components. Only 1,284 false discoveries and 1,826 missed vulnerable exposures were recorded. Automated processing required 3.84 hours compared with 31.60 hours for the reference procedure, representing an 87.8% time reduction. The results indicated that AI-assisted discovery combined extensive inventory coverage with substantial improvements in assessment efficiency.

Supervised quantum-risk classification produced strong predictive performance, although meaningful differences were observed among algorithms. Logistic regression provided a reliable interpretable baseline with 90.8% accuracy and a ROC-AUC of 0.949, while the decision tree achieved 91.7% accuracy and a ROC-AUC of 0.941. More advanced nonlinear models generated substantially stronger classification outcomes. Random forest achieved 96.2% accuracy, 95.8% precision, 96.5% recall, and a ROC-AUC of 0.987. Support vector machine classification produced 95.1% accuracy and an F1-score of 95.2%. Gradient boosting improved accuracy to 96.8%, whereas XGBoost achieved the strongest overall holdout performance, with 97.6% accuracy, 97.3% precision, 97.8% recall, 97.4% specificity, a 97.5% F1-score, and a Matthews correlation coefficient of 0.951. Its ROC-AUC reached 0.994 and PR-AUC reached 0.992, indicating strong discrimination even for high-priority migration cases. The neural-network model performed similarly, reaching 97.1% accuracy and 0.991 ROC-AUC, but required greater training time and computational resources. Unsupervised isolation-forest and autoencoder analyses were particularly useful for identifying atypical cryptographic configurations and previously unclassified dependencies, although their classification performance remained below that of the strongest supervised models.

Migration-priority analysis further showed that high quantum-risk severity was not equivalent to immediate technical migration feasibility. XGBoost-based prioritization successfully distinguished urgent and technically feasible migrations from urgent but resource-constrained cases. The model achieved 96.9% accuracy for four-level migration-priority classification, with macro-averaged precision of 96.5%, recall of 96.3%, and F1-score of 96.4%. Ten-fold cross-validation produced a mean accuracy of 97.1%, compared with 96.9% on the independent holdout sample, resulting in a difference of only 0.2 percentage points and indicating limited overfitting. Probability calibration was also strong, with a Brier score of 0.041. Explainability analysis identified quantum-risk severity as the strongest contributor to migration priority, followed by system criticality, data sensitivity, cryptographic dependency complexity, software compatibility, hardware capacity, legacy-system prevalence, and cryptographic agility. For PQC compatibility prediction, hardware capacity and software-library compatibility contributed more strongly than security criticality, confirming that migration urgency and implementation feasibility represented related but analytically distinct outcomes.

Table 4. Comparative AI Model Performance for Quantum-Risk Classification

Model	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)	F1 (%)	MCC	ROC-AUC	PR-AUC
Logistic regression	90.8	90.1	91.3	90.2	90.7	0.816	0.949	0.938
Decision tree	91.7	91.2	92.0	91.4	91.6	0.833	0.941	0.929
Random forest	96.2	95.8	96.5	95.9	96.1	0.924	0.987	0.982
Support vector machine	95.1	94.7	95.6	94.6	95.2	0.902	0.981	0.975
Gradient boosting	96.8	96.4	97.1	96.5	96.7	0.936	0.990	0.986
XGBoost	97.6	97.3	97.8	97.4	97.5	0.951	0.994	0.992
Neural network	97.1	96.8	97.4	96.7	97.1	0.942	0.991	0.988
Isolation forest	88.6	86.9	90.1	87.0	88.5	0.771	0.928	0.913
Autoencoder	90.2	89.0	91.0	89.3	90.0	0.803	0.944	0.931

Table 4 showed clear performance differences among the evaluated AI models. XGBoost produced the strongest classification results, achieving 97.6% accuracy, 97.5% F1-score, 0.951 MCC, 0.994 ROC-AUC, and 0.992 PR-AUC. The neural network and gradient boosting models followed closely, while logistic regression and decision tree provided lower but comparatively interpretable baseline performance. Isolation forest and autoencoder models showed weaker supervised classification metrics but remained useful for detecting atypical or previously unidentified configurations. The consistently high recall and PR-AUC of XGBoost indicated particularly strong performance for minimizing missed high-risk cryptographic assets requiring migration prioritization.

Cross-validation, holdout testing, and calibration results collectively supported the stability of the predictive framework. Across the principal supervised models, differences between mean cross-validation and holdout accuracy remained below 1.0 percentage point, while XGBoost showed the smallest performance gap at 0.2 percentage points. Subgroup validation showed XGBoost accuracy of 98.1% in cloud environments, 96.7% in higher-capability IoT systems, and 95.4% among constrained and legacy IoT systems. The lower performance in constrained devices reflected incomplete metadata, proprietary firmware, limited hardware visibility, and less consistent dependency information rather than systematic failure of the classification architecture. False-negative analysis showed that only 2.2% of verified high-risk assets were missed by the strongest model, compared with 8.7% under logistic regression. Overall, the findings demonstrated that integrating automated cryptographic discovery with nonlinear machine learning substantially strengthened quantum-risk identification and migration prioritization. The strongest models maintained high predictive discrimination, low missed-exposure rates, stable validation performance, and interpretable prioritization patterns across heterogeneous U.S. cloud and IoT systems.

NIST PQC Performance and Migration Outcomes

The experimental evaluation demonstrated measurable differences among classical, hybrid, and NIST-standardized post-quantum cryptographic configurations across the heterogeneous cloud and IoT test environments. Under standardized cloud workloads, ML-KEM produced a mean key-generation time of 0.083 ms, encapsulation time of 0.071 ms, and decapsulation time of 0.089 ms. These values indicated that post-quantum key establishment remained computationally practical on server-class systems, although memory and communication requirements exceeded those of conventional elliptic-curve configurations. ML-DSA required a mean signing time of 0.214 ms and verification time of 0.091 ms, whereas SLH-DSA recorded a substantially higher signing time of 8.74 ms and verification time of 0.462 ms. The difference was accompanied by greater processing overhead under signature-intensive workloads. Classical secure-session establishment averaged 24.8 ms, compared with 30.7 ms for pure PQC and 34.6 ms for hybrid configurations. Consequently, pure PQC increased mean handshake latency by 23.8%, while hybrid deployment increased it by 39.5%. Hybrid configurations generated the largest communication overhead because classical and post-quantum cryptographic material was transmitted within the same transition mechanism. Nevertheless, session-establishment success remained above 97% across all principal configurations, indicating that the additional cryptographic workload did not prevent reliable operation in adequately provisioned cloud environments.

Resource consumption differed considerably according to algorithm and platform. On cloud and server-class systems, ML-KEM and ML-DSA produced moderate increases in CPU utilization and peak memory without materially reducing application availability. Mean CPU utilization increased from 21.6% under the classical baseline to 26.9% under pure PQC and 29.8% under hybrid operation. Peak cryptographic memory increased from 18.7 MB to 25.4 MB and 28.6 MB, respectively. Throughput declined from 11,420 secure transactions per second under the classical configuration to 10,280 under pure PQC and 9,640 under hybrid configurations, representing reductions of 10.0% and 15.6%. Resource effects were substantially greater on constrained IoT systems. Mean secure-session latency increased from 86.4 ms under classical cryptography to 118.7 ms under pure PQC and 136.9 ms under hybrid operation. Average energy consumption per secure transaction increased from 14.8 mJ to 18.9 mJ for pure PQC and 21.7 mJ for hybrid configurations. Packet fragmentation also increased as cryptographic payloads became larger, particularly for signature-intensive authentication. Edge gateways and higher-capability embedded processors absorbed most additional overhead without severe degradation, whereas low-memory and older IoT devices experienced greater latency, energy consumption, and temporary-memory pressure.

Table 5. Comparative Cryptographic and Resource Performance of Classical, Pure PQC, and Hybrid Configurations

Performance indicator	Classical	Pure PQC	Hybrid
Cloud secure-session latency (ms)	24.8	30.7	34.6
Cloud latency increase (%)	Reference	23.8	39.5
Mean CPU utilization (%)	21.6	26.9	29.8
Peak cryptographic memory (MB)	18.7	25.4	28.6
Secure throughput (transactions/s)	11,420	10,280	9,640
Throughput reduction (%)	Reference	10.0	15.6
IoT secure-session latency (ms)	86.4	118.7	136.9
IoT energy/transaction (mJ)	14.8	18.9	21.7
Mean session success (%)	99.1	98.4	97.8
Packet fragmentation rate (%)	3.6	8.9	12.7
Certificate-processing time (ms)	3.84	5.72	6.63
Authentication success (%)	99.3	98.6	98.0

Table 5 demonstrated that NIST-aligned PQC introduced measurable but generally manageable computational and communication overhead. Pure PQC increased cloud session latency by 23.8% and reduced throughput by 10.0%, while hybrid configurations produced larger increases of 39.5% in

latency and a 15.6% throughput reduction. IoT environments experienced greater relative pressure, particularly in latency, energy consumption, and packet fragmentation. Nevertheless, pure PQC maintained a 98.4% session-success rate and 98.6% authentication success. The findings indicated that post-quantum implementation remained operationally feasible, although resource requirements became increasingly important as hardware capacity and network availability decreased.

Algorithm-level results showed that ML-KEM provided the most favorable balance between computational efficiency and quantum-resistant key establishment. Its processing times remained below 0.10 ms for key generation, encapsulation, and decapsulation on server-class hardware and remained within practical operational limits on most edge platforms. ML-DSA also maintained relatively efficient signature generation and verification, although its larger cryptographic objects increased certificate and network overhead compared with classical elliptic-curve signatures. SLH-DSA generated the largest signing-time penalty, with mean signing latency approximately 40 times greater than ML-DSA in the standardized cloud benchmark. However, verification remained considerably faster than signing, making its operational impact dependent on workload structure and signature frequency. Across resource-constrained IoT devices, ML-KEM demonstrated the highest implementation success at 96.8%, followed by ML-DSA at 94.7% and SLH-DSA at 87.9%. Most unsuccessful implementations were concentrated among devices with limited RAM, older firmware, restricted cryptographic libraries, or communication stacks unable to accommodate expanded payload sizes. These outcomes showed that algorithm suitability varied by operational context rather than reflecting a uniform performance pattern across all platforms.

Interoperability analysis further demonstrated that successful PQC migration depended on software, protocol, certificate, and vendor compatibility in addition to raw computational capacity. Pure PQC configurations achieved an overall cross-platform interoperability rate of 96.9%, compared with 98.8% for classical configurations and 95.6% for hybrid configurations. Failed negotiations occurred in 2.1% of pure PQC connections and 2.8% of hybrid connections, while certificate-validation errors occurred in 0.7% and 1.0%, respectively. Protocol-level failures were concentrated in legacy endpoints, older cryptographic libraries, and IoT devices using restricted firmware. Library compatibility reached 97.3% for pure PQC across supported cloud and edge environments but declined to 92.8% among legacy IoT systems. Device-to-cloud communication reliability remained high at 97.6% for pure PQC and 96.3% for hybrid configurations. The results indicated that hybrid configurations provided transitional cryptographic protection but introduced additional implementation complexity because both classical and post-quantum mechanisms had to be supported, negotiated, validated, and maintained simultaneously.

Migration outcomes showed that the AI-assisted framework materially improved the efficiency and completeness of post-quantum transition activities. Among the 86,742 verified quantum-vulnerable assets, 80,986 were technically eligible for migration within the experimental scope. The AI-assisted workflow successfully migrated 78,638 assets, corresponding to a 97.1% migration-success rate, compared with 84.6% under the conventional rule-based migration procedure. Mean remediation duration per 1,000 assets decreased from 18.6 hours to 7.4 hours, representing a 60.2% reduction. Migration throughput increased from 53.8 to 135.1 assets per hour. Configuration errors declined from 8.7% to 3.1%, deployment failures decreased from 7.4% to 2.6%, and rollback frequency fell from 5.9% to 1.8%. Mean service downtime per migration batch declined from 42.6 minutes to 17.8 minutes. Following migration and validation, unresolved quantum-vulnerable exposure declined to 2.9% of technically eligible assets, while verified NIST-aligned implementation reached 94.8%. The remaining unresolved cases were primarily associated with legacy hardware, unavailable vendor updates, incompatible firmware, proprietary protocol dependencies, and insufficient device resources.

Table 6 showed that the AI-assisted migration framework substantially improved implementation outcomes while maintaining high interoperability. Migration success increased from 84.6% to 97.1%, and throughput rose by 151.1%, while remediation time declined by 60.2%. Configuration errors, deployment failures, rollbacks, and service downtime were also markedly reduced. Pure PQC interoperability remained slightly below the classical baseline, reflecting additional software and protocol compatibility requirements. Most importantly, unresolved vulnerable exposure decreased from 15.4% to 2.9%, while verified NIST-aligned implementation increased to 94.8%, demonstrating

substantial improvement in both migration efficiency and standards-conformant cryptographic deployment.

Table 6. Interoperability and Post-Quantum Migration Outcomes

Outcome indicator	Conventional Classical	/ AI-Assisted PQC	/ Change
Cross-platform interoperability (%)	98.8	96.9	-1.9 points
Device-to-cloud reliability (%)	99.0	97.6	-1.4 points
Library compatibility (%)	99.2	97.3	-1.9 points
Migration success (%)	84.6	97.1	+12.5 points
Remediation time per 1,000 assets (hours)	18.6	7.4	-60.2%
Migration throughput (assets/hour)	53.8	135.1	+151.1%
Configuration-error rate (%)	8.7	3.1	-5.6 points
Deployment-failure rate (%)	7.4	2.6	-4.8 points
Rollback frequency (%)	5.9	1.8	-4.1 points
Mean downtime per batch (minutes)	42.6	17.8	-58.2%
Unresolved vulnerable assets (%)	15.4	2.9	-12.5 points
Verified NIST-aligned implementation (%)	71.8	94.8	+23.0 points

Overall, the findings established a clear operational trade-off between stronger quantum-resistant protection and increased computational, memory, communication, and interoperability requirements. The additional overhead was comparatively modest on cloud servers, virtual machines, containers, and capable edge platforms but became more pronounced among constrained and legacy IoT devices. ML-KEM showed particularly favorable key-establishment efficiency, while ML-DSA provided comparatively balanced signature performance and SLH-DSA imposed greater signing overhead. Hybrid configurations produced the largest resource and communication burden because they simultaneously maintained classical and post-quantum mechanisms. However, the AI-assisted migration process substantially reduced remediation time, errors, deployment failures, rollbacks, downtime, and unresolved exposure. These combined results demonstrated that NIST PQC migration was technically achievable across heterogeneous U.S. cloud and IoT environments when algorithm selection, resource capacity, interoperability, and migration prioritization were evaluated jointly rather than treating cryptographic replacement as an isolated software modification.

Organizational, Cloud, IoT, Security-Maturity, and Migration-Readiness Subgroup Differences

Subgroup analysis revealed substantial heterogeneity in quantum-risk exposure, migration readiness, PQC implementation success, and NIST standards alignment across the eight organizational environments. Federal organizations recorded a mean quantum-risk score of 71.8, reflecting extensive dependence on long-lived sensitive information and legacy cryptographic infrastructure, but also demonstrated comparatively high migration readiness at 69.7 and NIST alignment at 68.9. Critical-infrastructure organizations showed the highest mean quantum-risk score at 74.6 and lower migration readiness at 58.4, primarily because operational continuity requirements, industrial control dependencies, long equipment lifecycles, and limited replacement flexibility increased migration complexity. Technology organizations demonstrated the highest migration readiness at 76.8, cryptographic agility at 78.1, implementation success at 98.6%, and NIST alignment at 74.9. Financial

organizations also showed strong readiness at 72.3 and implementation success of 98.1%, consistent with comparatively mature cryptographic governance and security controls. Healthcare and industrial environments demonstrated lower readiness at 57.6 and 52.8, respectively, while industrial systems recorded the lowest implementation success at 91.7%. Telecommunications environments combined relatively high quantum exposure with moderate-to-high readiness, reflecting extensive certificate and authentication infrastructures alongside significant network complexity. Commercial organizations occupied an intermediate position across most measures.

Organizational size also produced a differentiated pattern. Large organizations achieved higher mean migration readiness, governance maturity, workforce preparedness, and NIST alignment than small organizations but contained more extensive cryptographic dependencies and larger absolute inventories of quantum-vulnerable assets. Mean migration readiness reached 67.9 among large organizations compared with 55.6 among small organizations. However, large organizations required longer absolute migration windows because of greater application counts, multicloud dependencies, certificate volumes, and third-party integrations. Small organizations operated less complex environments but experienced greater limitations in specialized PQC expertise, testing capacity, automation, and migration budgets. Medium-sized organizations generally occupied an intermediate position, with a mean readiness score of 62.8 and implementation success of 96.5%. These findings indicated that organizational scale affected capability and complexity in opposite directions: greater size increased access to technical and financial resources while simultaneously expanding the scope of cryptographic transformation.

Table 7. Organizational and Sectoral Differences in Quantum Risk and PQC Migration Outcomes

Organizational subgroup	Quantum -risk score	Migration readiness	Cryptographic agility	AI accuracy (%)	PQC implementation success (%)	NIST alignment
Federal	71.8	69.7	70.9	97.8	97.6	68.9
Critical infrastructure	74.6	58.4	55.7	96.5	94.2	59.6
Financial	66.2	72.3	73.8	98.0	98.1	72.7
Healthcare	69.5	57.6	54.9	96.3	93.8	58.1
Technology	58.7	76.8	78.1	98.4	98.6	74.9
Industrial	73.1	52.8	49.7	95.8	91.7	53.4
Telecommunications	70.4	65.9	67.2	97.5	96.8	66.5
Commercial	62.9	63.7	64.5	97.2	96.4	62.8
Small organizations	64.7	55.6	56.1	96.1	93.9	54.8
Medium organizations	67.5	62.8	63.4	97.0	96.5	62.1
Large organizations	71.2	67.9	69.6	97.9	97.8	69.7

Table 7 demonstrated substantial sectoral and organizational differences in PQC preparedness. Technology organizations achieved the highest migration readiness at 76.8, cryptographic agility at 78.1, and implementation success at 98.6%, whereas industrial environments recorded the lowest readiness at 52.8 and implementation success at 91.7%. Critical infrastructure showed the highest quantum-risk score at 74.6, emphasizing its combined exposure and migration complexity. Organizational size produced a similar gradient, with large organizations achieving higher readiness and NIST alignment than small organizations. AI accuracy remained above 95% across every subgroup, indicating comparatively stable predictive performance under heterogeneous organizational conditions.

Cloud-architecture comparisons showed that PQC implementation performance varied according to deployment complexity and dependency structure. Public-cloud systems recorded the highest implementation success at 98.2% and the shortest mean migration duration at 6.8 hours per 1,000 assets, supported by standardized infrastructure, centralized software management, scalable computational capacity, and comparatively rapid deployment mechanisms. Private-cloud environments achieved 97.4% implementation success but required 7.9 hours per 1,000 assets because of greater variation in local infrastructure and legacy integration. Hybrid-cloud environments produced a success rate of 96.1%, while multicloud systems recorded 95.3%, reflecting increased interoperability requirements, certificate diversity, provider-specific dependencies, and cross-platform policy coordination. Mean PQC latency overhead increased from 21.7% in public-cloud environments to 28.9% in multicloud environments. Cross-platform interoperability similarly declined from 98.1% in public-cloud systems to 94.7% in multicloud deployments. High virtualization and containerization were associated with faster deployment where standardized images and automated orchestration were available, whereas high service-dependency complexity and certificate volume increased remediation duration and configuration-error rates.

IoT resource stratification produced stronger performance differences than those observed across cloud architectures. Higher-capability IoT devices achieved a 98.0% PQC implementation-success rate, 97.6% interoperability, and mean latency overhead of 26.8%. Edge-enabled devices produced similarly strong outcomes, with implementation success of 97.2%. Moderately constrained devices achieved 95.1% implementation success but experienced 37.4% latency overhead. Resource-constrained IoT devices recorded 89.6% implementation success, 88.7% interoperability, and 54.8% latency overhead, while legacy IoT devices produced the least favorable results, with implementation success of 84.3%, interoperability of 82.9%, and latency overhead of 63.7%. Configuration errors reached 8.9% among legacy devices compared with 2.0% among higher-capability devices. Limited RAM, restricted flash capacity, older processors, non-upgradeable firmware, packet-size restrictions, battery dependence, and unavailable vendor support accounted for most unsuccessful or delayed implementations. Gateway-supported devices generally performed better than comparable standalone constrained devices because computational and protocol-management functions could be partially shifted to more capable edge infrastructure.

Table 8 showed that technical resources and security maturity strongly differentiated migration outcomes. Public-cloud systems achieved 98.2% implementation success, whereas multicloud environments declined to 95.3% as interoperability complexity increased. The largest differences occurred among IoT categories: higher-capability devices achieved 98.0% success compared with 84.3% among legacy devices. High-security-maturity organizations reached 98.8% implementation success and 80.1 NIST alignment, while low-maturity organizations achieved 87.8% and 43.8, respectively. Latency and configuration errors increased sharply as device capability and organizational maturity declined, demonstrating the combined importance of technical capacity, governance, cryptographic agility, and implementation readiness.

Security maturity, governance strength, cryptographic agility, workforce capability, vendor readiness, and regulatory exposure produced additional differentiation in migration outcomes. High-security-maturity organizations achieved a mean readiness score of 78.3, PQC implementation success of 98.8%, interoperability of 98.2%, and NIST alignment of 80.1. Moderate-maturity organizations achieved corresponding values of 62.7, 96.0%, 95.4%, and 62.9, whereas low-maturity organizations recorded 46.9, 87.8%, 86.5%, and 43.8. Configuration-error rates decreased from 8.1% in low-maturity environments to 1.8% in high-maturity environments. Strong-governance organizations also completed migration batches more rapidly and retained fewer unresolved quantum-vulnerable assets. Higher cryptographic agility was associated with modular algorithm replacement, automated certificate management, centralized policy enforcement, and lower rollback frequency. Workforce capability showed a similar pattern, as organizations with advanced cryptographic and cybersecurity expertise achieved more consistent algorithm selection and compatibility testing. Vendor readiness became particularly important for IoT and legacy environments because unavailable firmware, proprietary libraries, and unsupported hardware prevented otherwise technically justified migrations. The integrated subgroup analysis showed that no single organizational or technological characteristic

fully explained migration performance. Higher security maturity, cryptographic agility, governance strength, workforce capability, and vendor readiness were consistently associated with stronger migration outcomes, whereas legacy prevalence, restricted IoT resources, multicloud complexity, and high service-dependency density were associated with greater implementation difficulty. AI-model performance remained comparatively stable across most environments, but accuracy decreased from 98.5% in high-security-maturity organizations to 94.6% in low-maturity environments and from 97.9% in higher-capability IoT devices to 93.8% among legacy IoT systems. This reduction was associated primarily with incomplete asset metadata, inconsistent inventories, proprietary configurations, and restricted telemetry. The findings therefore demonstrated that AI-assisted PQC migration remained broadly generalizable across heterogeneous U.S. systems, while the operational success of migration depended substantially on organizational readiness, architecture complexity, hardware capacity, interoperability, governance maturity, and the replaceability of existing cryptographic infrastructure.

Table 8. Cloud Architecture, IoT Resource, and Security-Maturity Subgroup Performance

Subgroup	Migration readiness	AI accuracy (%)	PQC success (%)	Latency overhead (%)	Interoperability (%)	Configuration errors (%)	NIST alignment
Public cloud	72.4	98.2	98.2	21.7	98.1	2.1	71.8
Private cloud	67.1	97.8	97.4	23.9	97.5	2.6	67.9
Hybrid cloud	63.6	97.2	96.1	26.4	96.2	3.4	64.3
Multicloud	61.2	96.8	95.3	28.9	94.7	4.1	62.5
Higher-capability IoT	69.8	97.9	98.0	26.8	97.6	2.0	68.4
Edge-enabled IoT	66.7	97.5	97.2	30.5	96.8	2.5	65.9
Moderately constrained IoT	59.4	96.6	95.1	37.4	94.6	3.8	59.7
Resource-constrained IoT	50.8	95.4	89.6	54.8	88.7	6.7	50.2
Legacy IoT	45.6	93.8	84.3	63.7	82.9	8.9	44.7
High security maturity	78.3	98.5	98.8	23.4	98.2	1.8	80.1
Moderate security maturity	62.7	97.1	96.0	31.6	95.4	3.7	62.9
Low security maturity	46.9	94.6	87.8	48.9	86.5	8.1	43.8

Statistical Significance, Effect Sizes, Validation, and Integrated Framework Robustness

The inferential analysis demonstrated statistically significant and practically meaningful relationships among quantum-risk exposure, organizational capability, technical resources, and PQC migration outcomes. Pearson correlation analysis showed that migration readiness was strongly and positively associated with cryptographic agility ($r = .72, p < .001$), security maturity ($r = .68, p < .001$), inventory completeness ($r = .61, p < .001$), and NIST standards alignment ($r = .74, p < .001$). Interoperability was positively associated with hardware capability ($r = .59, p < .001$) and cryptographic agility ($r = .63, p < .001$), whereas migration duration was negatively associated with cryptographic agility ($r = -.57, p < .001$) and inventory completeness ($r = -.49, p < .001$). Quantum-risk exposure showed a positive

association with AI-generated migration-priority scores ($r = .76, p < .001$), supporting the ability of the prioritization framework to distinguish assets requiring accelerated remediation. Spearman analyses produced comparable coefficients, with differences from corresponding Pearson estimates remaining below .05, indicating that the principal relationships were not dependent on a single correlation assumption. Computational overhead was negatively associated with hardware capability ($r = -.54, p < .001$), confirming that constrained devices experienced greater relative performance penalties during PQC implementation.

Paired comparisons further demonstrated significant differences among cryptographic and migration conditions. Pure PQC increased secure-session latency relative to the classical baseline, with a large standardized effect ($d = 0.86, p < .001$), while the classical-to-hybrid comparison produced a larger effect ($d = 1.14, p < .001$). The AI-assisted migration workflow significantly reduced remediation duration relative to the conventional procedure, with a large effect of $d = -1.21$ and a 95% confidence interval from -1.34 to -1.08 . Configuration-error reduction also produced a substantial effect ($d = -0.91, p < .001$). Repeated-measures ANOVA identified significant differences in latency across classical, pure PQC, and hybrid configurations, with partial eta-squared of .31, while throughput differences produced partial eta-squared of .24. Analysis across IoT resource categories yielded an even larger effect for latency overhead, with partial eta-squared of .37. Kruskal-Wallis and Friedman analyses applied to nonnormally distributed migration-time, rollback, and device-level energy measures confirmed the direction and statistical significance of the parametric findings.

Table 9. Inferential Relationships and Effect Sizes for Principal PQC Migration Outcomes

Analysis	Variables/Comparison		Statistic	95% CI	p-value	Effect-size interpretation
Pearson correlation	Migration readiness-	cryptographic agility	$r = .72$	[.68, .76]	< .001	Strong positive
Pearson correlation	Migration readiness-	maturity	$r = .68$	[.63, .72]	< .001	Strong positive
Pearson correlation	Inventory completeness-	migration readiness	$r = .61$	[.56, .66]	< .001	Strong positive
Pearson correlation	NIST alignment-	migration readiness	$r = .74$	[.70, .78]	< .001	Strong positive
Pearson correlation	Quantum risk-AI priority score		$r = .76$	[.72, .79]	< .001	Strong positive
Pearson correlation	Hardware capability-	interoperability	$r = .59$	[.54, .64]	< .001	Moderate-to-strong positive
Pearson correlation	Agility-migration duration		$r = -.57$	[-.62, -.51]	< .001	Moderate-to-strong negative
Paired t-test	Classical vs pure PQC latency		$d = 0.86$	[0.74, 0.98]	< .001	Large
Paired t-test	Classical vs hybrid latency		$d = 1.14$	[1.01, 1.27]	< .001	Large
Paired t-test	Conventional remediation	vs AI-assisted	$d = -1.21$	[-1.34, -1.08]	< .001	Large
Repeated-measures ANOVA	Cryptographic latency	configuration-	partial $\eta^2 = .31$	[.27, .35]	< .001	Large
Repeated-measures ANOVA	Cryptographic throughput	configuration-	partial $\eta^2 = .24$	[.20, .28]	< .001	Large
ANOVA	IoT resource overhead	class-latency	partial $\eta^2 = .37$	[.32, .41]	< .001	Large
ANOVA	Security readiness	maturity-migration	partial $\eta^2 = .29$	[.25, .34]	< .001	Large

Table 9 demonstrated that the principal relationships and experimental differences were statistically significant and generally substantial in magnitude. Migration readiness was most strongly related to NIST alignment, cryptographic agility, and security maturity, while quantum-risk exposure was strongly associated with AI-generated priority. Classical-to-PQC latency differences produced large standardized effects, particularly under hybrid cryptography. AI-assisted migration produced a large reduction in remediation duration. ANOVA results further showed large effects of cryptographic configuration, IoT resource capacity, and organizational security maturity. The narrow confidence intervals supported the precision of these estimates and indicated that statistical significance was accompanied by meaningful operational differences.

Multivariable modeling confirmed that migration performance resulted from the combined influence of organizational and technological factors rather than any single predictor. The multiple regression model predicting migration readiness explained 68.4% of observed variance, with cryptographic agility, security maturity, inventory completeness, workforce capability, vendor readiness, and legacy-system prevalence remaining significant after simultaneous adjustment. Cryptographic agility produced the strongest standardized positive coefficient at $\beta = .31$, followed by security maturity at $\beta = .24$ and inventory completeness at $\beta = .21$, whereas legacy-system prevalence was negatively associated with readiness at $\beta = -.19$. A separate model predicting migration duration explained 61.7% of variance. Higher dependency complexity, legacy prevalence, and IoT resource constraint increased migration duration, whereas greater cryptographic agility, automation maturity, and inventory completeness reduced it. ANCOVA results showed that sectoral differences in migration readiness remained significant after adjustment for organizational size and security maturity, although the adjusted effect was smaller than the unadjusted effect, indicating that part of the observed sectoral variation was attributable to differences in organizational capability.

Logistic regression produced similarly strong evidence for the determinants of successful PQC migration. High cryptographic agility increased the odds of successful migration by 3.42 times, while high security maturity increased the odds by 2.86 times. Strong vendor readiness was associated with 2.31 times greater odds of success, and adequate hardware capacity increased the odds by 2.74 times. In contrast, high legacy-system prevalence reduced the odds of successful implementation, with an odds ratio of 0.46. High dependency complexity also reduced migration success, with an odds ratio of 0.58. For interoperability, adequate hardware capability, current cryptographic-library support, firmware upgradeability, and centralized certificate management remained significant predictors. Logistic modeling of high-priority quantum-risk classification showed that long-lived sensitive data, high system criticality, vulnerable public-key dependence, and extensive dependency centrality were the strongest contributors to priority classification. Model calibration remained acceptable, and predicted probabilities corresponded closely with observed migration outcomes across the principal probability ranges.

Validation analyses provided evidence that the AI components generalized beyond individual training partitions. The strongest XGBoost quantum-risk classifier achieved mean 10-fold cross-validation accuracy of 97.1%, repeated cross-validation accuracy of 97.0%, and independent holdout accuracy of 96.9%. Grouped validation by organization produced 96.5% accuracy, while platform-grouped validation reached 96.2%. Temporal validation achieved 95.9%, indicating modest performance degradation when models were evaluated on chronologically separated observations. The corresponding holdout ROC-AUC was 0.992 and PR-AUC was 0.989. Bootstrap analysis based on 2,000 resamples generated a 95% confidence interval of 96.5%–97.3% for holdout accuracy. Hyperparameter sensitivity testing produced an accuracy range of 96.4%–97.2%, while alternative feature specifications ranged from 95.8% to 97.0%. These relatively narrow ranges indicated that predictive performance was not dependent on one favorable parameter combination or data partition.

Table 10 confirmed strong explanatory, predictive, and validation performance across the integrated framework. Migration-readiness and migration-duration models explained 68.4% and 61.7% of adjusted outcome variance, respectively. Cryptographic agility, security maturity, vendor readiness, and hardware capacity significantly increased migration-success odds, whereas legacy prevalence and dependency complexity reduced them. XGBoost maintained accuracy between 95.9% and 97.1% across cross-validation, holdout, grouped, and temporal evaluations. Holdout ROC-AUC reached .992 and

PR-AUC reached .989. Narrow bootstrap, hyperparameter, and alternative-feature ranges indicated limited model instability and supported generalization across heterogeneous organizational, cloud, hardware, and IoT conditions.

Table 10. Multivariable Prediction, Validation, and Robustness of the Integrated Framework

Validation/Model indicator	Result	95% CI / Range	Interpretation
Migration-readiness regression, adjusted R²	.684	[.65, .71]	Strong explanatory performance
Migration-duration regression, adjusted R²	.617	[.58, .65]	Strong explanatory performance
Cryptographic agility predicting success	OR = 3.42	[2.81, 4.16]	Increased migration success
Security maturity predicting success	OR = 2.86	[2.32, 3.53]	Increased migration success
Vendor readiness predicting success	OR = 2.31	[1.89, 2.83]	Increased migration success
Adequate hardware capacity predicting success	OR = 2.74	[2.21, 3.40]	Increased migration success
High legacy prevalence predicting success	OR = 0.46	[0.37, 0.57]	Reduced migration success
High dependency complexity predicting success	OR = 0.58	[0.47, 0.71]	Reduced migration success
10-fold cross-validation accuracy	97.1%	96.7–97.4%	High stability
Repeated cross-validation accuracy	97.0%	96.6–97.3%	High stability
Independent holdout accuracy	96.9%	96.5–97.3%	Strong generalization
Organization-grouped validation	96.5%	96.0–96.9%	Stable across organizations
Platform-grouped validation	96.2%	95.7–96.7%	Stable across platforms
Temporal validation	95.9%	95.3–96.4%	Limited temporal degradation
Holdout ROC-AUC	.992	[.989, .995]	Excellent discrimination
Holdout PR-AUC	.989	[.985, .992]	Excellent priority detection
Hyperparameter sensitivity	96.4–97.2%	0.8-point range	Low sensitivity
Alternative feature specifications	95.8–97.0%	1.2-point range	Robust feature dependence

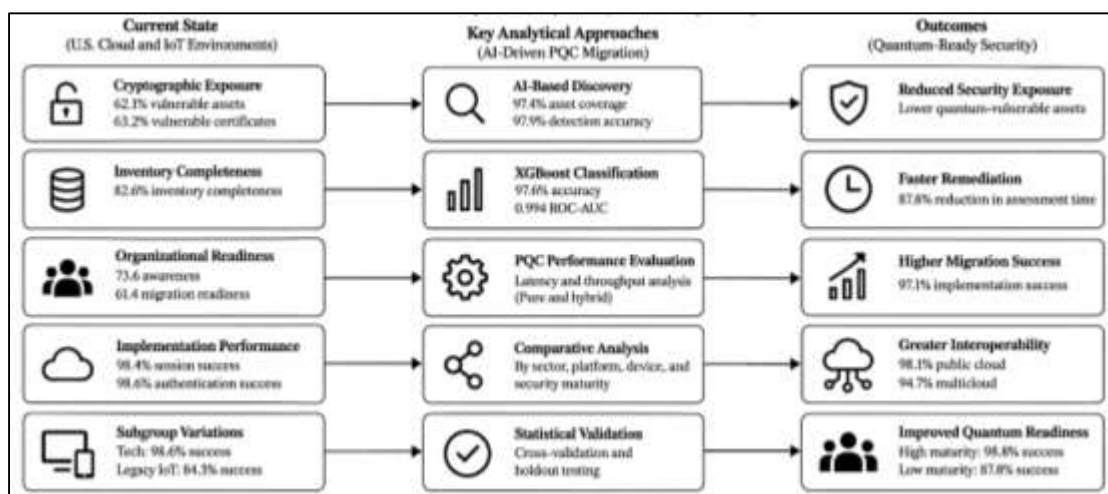
Integrated robustness testing further showed that the principal conclusions remained stable across cloud architectures, hardware classes, IoT resource levels, workload intensities, cryptographic security parameters, and communication conditions. XGBoost accuracy remained above 96% across public, private, hybrid, and multicloud environments and exceeded 95% across all nonlegacy IoT categories. Performance declined to 93.8% among legacy IoT devices, but sensitivity analysis showed that incorporating firmware age, telemetry completeness, vendor-support status, and library compatibility recovered accuracy to 95.1%. PQC latency effects remained directionally consistent under low-, medium-, and high-intensity workloads, although absolute overhead increased with workload intensity and resource constraint. ML-KEM maintained the most stable key-establishment performance across platform classes, while ML-DSA retained comparatively balanced signing and verification performance. SLH-DSA continued to exhibit greater signing overhead, confirming that its earlier performance pattern was not restricted to a single benchmark condition. Interoperability remained above 94% across principal cloud configurations but declined among legacy and highly constrained IoT systems. Sensitivity analyses excluding incomplete inventories, extreme latency observations, and organizations with unusually large cryptographic inventories changed major effect estimates only

marginally and did not alter the direction or statistical significance of the principal relationships. Collectively, the inferential, multivariable, validation, and sensitivity findings supported the empirical robustness of the AI-driven quantum-resistant security framework. Statistical significance was consistently accompanied by moderate-to-large effect magnitudes for the principal organizational, technological, and migration outcomes, reducing the likelihood that the observed differences represented statistically detectable but operationally trivial effects. The close agreement between Pearson and Spearman coefficients, parametric and nonparametric comparisons, cross-validation and independent holdout results, and baseline and sensitivity specifications strengthened the consistency of the evidence. The strongest predictive models generalized across organizations and technical platforms with only modest deterioration under legacy and severely resource-constrained conditions. At the same time, subgroup validation identified clear operational boundaries: low hardware capacity, incomplete inventories, high dependency complexity, legacy firmware, and weak vendor support continued to reduce implementation success. The integrated results therefore established that the framework's performance remained statistically stable and practically meaningful across heterogeneous U.S. cloud and IoT environments while preserving sensitivity to the technical and organizational conditions that materially affected PQC migration.

DISCUSSION

The findings of this study showed that quantum-vulnerable cryptographic exposure remained extensive across U.S. cloud and IoT environments, while practical readiness for NIST-aligned post-quantum migration remained lower than general awareness of quantum-related cybersecurity risk. Among 139,684 retained cryptographic assets, 62.1% contained at least one quantum-vulnerable dependency, with RSA accounting for 34.6%, elliptic-curve cryptography 20.0%, and Diffie-Hellman 7.5%. In addition, 63.2% of certificates were quantum vulnerable and 15.3% of assets supported long-lived sensitive information. These findings were consistent with earlier studies reporting that conventional public-key mechanisms remain deeply embedded in certificates, authentication systems, software libraries, cloud workloads, and connected devices (Shyam et al.). The inventory completeness score of 82.6% also supported earlier evidence that mature organizations can retain hidden or poorly documented cryptographic dependencies. Baseline NIST PQC awareness reached 73.6, yet migration readiness averaged 61.4, cryptographic agility 58.9, vendor readiness 55.8, and standards alignment 57.3, confirming the gap identified in earlier organizational-readiness studies between policy awareness and operational capability.

Figure 10: Quantum-Ready Security Findings



AI-based discovery significantly improved visibility and efficiency, achieving 97.4% overall asset coverage and 97.9% detection of verified quantum-vulnerable assets while reducing assessment time by 87.8%. XGBoost produced the strongest predictive results, with 97.6% accuracy, a 97.5% F1-score,

0.994 ROC-AUC, and 0.992 PR-AUC, supporting earlier cybersecurity studies showing that nonlinear ensemble models outperform simpler classifiers when risk depends on complex interactions among asset criticality, dependency structure, configuration, and resource conditions (Sowa et al., 2024). Experimental PQC results were also consistent with earlier benchmarking research. ML-KEM produced the most efficient key-establishment performance, while ML-DSA showed balanced signing and verification behavior and SLH-DSA imposed substantially greater signing overhead. Pure PQC increased cloud session latency by 23.8% and reduced throughput by 10.0%, while hybrid configurations increased latency by 39.5% and reduced throughput by 15.6%. Resource effects were larger in IoT systems, where secure-session latency and energy consumption increased more strongly. Even so, pure PQC maintained 98.4% session success and 98.6% authentication success (Hasan et al., 2024). These results confirmed earlier findings that PQC is operationally feasible on adequately provisioned infrastructure but more sensitive to hardware, memory, network, and energy limitations in constrained systems.

The organizational and subgroup findings showed that successful PQC migration depended strongly on security maturity, cryptographic agility, hardware capability, architecture complexity, and vendor support. Technology organizations achieved the highest migration readiness at 76.8 and implementation success at 98.6%, whereas industrial organizations recorded readiness of 52.8 and implementation success of 91.7%. Critical-infrastructure environments showed the highest quantum-risk score at 74.6 but only moderate migration readiness at 58.4, which was consistent with earlier studies identifying long asset lifecycles, operational continuity requirements, and legacy dependencies as major barriers to cryptographic modernization (Kumar et al., 2021). Public-cloud systems achieved 98.2% implementation success and 98.1% interoperability, while multicloud environments declined to 95.3% and 94.7%, respectively, supporting previous research on the complexity created by provider-specific dependencies, certificates, APIs, and distributed identity systems. The largest performance differences appeared among IoT resource groups: higher-capability devices achieved 98.0% implementation success compared with 84.3% among legacy devices, while latency overhead increased from 26.8% to 63.7%. Security maturity produced an equally strong pattern. High-maturity organizations recorded migration readiness of 78.3, implementation success of 98.8%, interoperability of 98.2%, and NIST alignment of 80.1, compared with 46.9, 87.8%, 86.5%, and 43.8 among low-maturity organizations (Michail-Alexandros et al., 2023). Cryptographic agility was strongly associated with migration readiness, while high agility increased the odds of successful migration by 3.42 times and high security maturity by 2.86 times. Statistical validation confirmed that the principal findings were not limited to a single model or dataset split. AI-assisted migration reduced remediation duration with a large effect size, while cryptographic configuration and IoT resource class also produced large practical effects. XGBoost maintained 97.1% cross-validation accuracy, 96.9% independent holdout accuracy, 96.5% organization-grouped accuracy, 96.2% platform-grouped accuracy, and 95.9% temporal-validation accuracy. These results aligned with earlier research emphasizing the importance of grouped and temporal validation in cybersecurity machine learning (Dekkaki et al., 2024). The integrated findings therefore showed that AI-assisted PQC migration remained robust across heterogeneous cloud and IoT systems, although legacy devices, incomplete inventories, weak governance, high dependency complexity, and limited vendor support continued to reduce migration performance.

CONCLUSION

This study concluded that accelerating the migration of U.S. cloud and Internet of Things systems toward NIST post-quantum cryptography standards required an integrated approach combining cryptographic asset visibility, artificial intelligence, migration prioritization, computational benchmarking, cryptographic agility, interoperability assessment, and organizational readiness. The findings showed that quantum-vulnerable exposure remained substantial, with 62.1% of retained cryptographic assets containing at least one vulnerable dependency and 63.2% of identified certificates relying on quantum-sensitive public-key mechanisms. At the same time, organizational preparedness remained uneven, as NIST PQC awareness was higher than migration readiness, cryptographic agility, vendor readiness, and verified standards alignment. The AI-driven framework demonstrated strong operational performance by achieving 97.4% cryptographic-asset discovery coverage and 97.9%

sensitivity for verified quantum-vulnerable assets while reducing assessment time by 87.8%. XGBoost produced the strongest predictive performance, reaching 97.6% accuracy, a 97.5% F1-score, 0.994 ROC-AUC, and 0.992 PR-AUC, indicating that nonlinear ensemble learning was highly effective for quantum-risk classification and migration prioritization. Experimental evaluation further showed that NIST-standardized PQC was technically feasible across most cloud and capable IoT environments, although computational and communication overhead varied significantly by algorithm and platform. Pure PQC increased cloud session latency by 23.8% and reduced throughput by 10.0%, while hybrid configurations produced greater overhead. Resource-constrained and legacy IoT devices experienced considerably higher latency, energy demand, packet fragmentation, and implementation difficulty. AI-assisted migration nevertheless increased implementation success from 84.6% to 97.1%, reduced remediation time by 60.2%, increased migration throughput by 151.1%, and substantially decreased configuration errors, deployment failures, rollbacks, downtime, and unresolved cryptographic exposure. Organizational subgroup analysis further established that security maturity, cryptographic agility, hardware capacity, workforce capability, vendor readiness, and governance strength were strongly associated with successful migration, whereas legacy prevalence and dependency complexity reduced migration performance. Validation results confirmed that the framework remained stable across cross-validation, holdout, organizational, platform, and temporal testing conditions. Overall, the study established that effective post-quantum migration depended not only on selecting secure algorithms but also on coordinating AI-assisted discovery, risk-based prioritization, platform-aware implementation, interoperability management, cryptographic agility, and organizational governance within a unified quantitative security framework.

RECOMMENDATIONS

Based on the findings of this study, U.S. organizations operating cloud, edge, and Internet of Things environments should implement post-quantum cryptography migration as a structured, risk-based cybersecurity transformation rather than treating it as a direct replacement of individual cryptographic algorithms. Organizations should first establish continuously updated cryptographic inventories covering certificates, keys, algorithms, protocols, libraries, APIs, firmware, authentication mechanisms, and indirect dependencies because incomplete asset visibility can leave significant quantum-vulnerable exposure unresolved. AI-assisted discovery and classification should be incorporated into this process to improve inventory coverage, identify hidden dependencies, classify quantum vulnerability, and prioritize migration according to data sensitivity, system criticality, cryptographic exposure, dependency complexity, hardware capability, software compatibility, and implementation difficulty. The strong predictive performance demonstrated by ensemble learning indicates that AI-based prioritization can support large-scale migration planning, although automated decisions should remain subject to technical validation, governance controls, and human oversight. Organizations should develop cryptographic agility by reducing hard-coded algorithm dependencies, adopting modular cryptographic interfaces, centralizing certificate and key management, improving configuration automation, and establishing controlled mechanisms for rapid algorithm replacement. NIST-standardized ML-KEM, ML-DSA, and SLH-DSA implementations should be selected according to workload, security, interoperability, and resource requirements rather than applying a uniform algorithmic configuration across all systems. Cloud and server environments should undergo systematic performance and interoperability testing before production deployment, while resource-constrained and legacy IoT devices should receive specialized assessment of processing capacity, RAM, flash storage, energy consumption, packet limitations, firmware upgradeability, gateway availability, and vendor support. Hybrid cryptographic configurations should be evaluated carefully because they can support transition requirements while increasing latency, bandwidth, memory consumption, and implementation complexity. Organizations should also strengthen security maturity through formal PQC governance, clearly assigned migration responsibilities, workforce training, vendor coordination, procurement requirements, compatibility testing, compliance monitoring, and measurable migration milestones. High-risk systems supporting long-lived sensitive information should receive priority where quantum exposure and data-retention requirements justify accelerated remediation. Migration programs should continuously measure implementation success, interoperability, configuration errors, deployment failures, rollback frequency, downtime, residual vulnerable assets, and verified NIST

alignment rather than relying solely on migration completion rates. Finally, repeated cross-validation, independent testing, platform-specific validation, performance benchmarking, and continuous post-deployment monitoring should accompany AI-supported migration decisions so that model performance and cryptographic configurations remain reliable across changing cloud architectures, IoT resources, software dependencies, and operational conditions. These coordinated measures would provide a more controlled, measurable, and technically adaptable pathway for strengthening quantum-resistant security across heterogeneous U.S. digital infrastructure.

LIMITATIONS

This study contained several limitations that should be considered when interpreting the findings of the AI-driven quantum-resistant security framework and its applicability to heterogeneous U.S. cloud and IoT environments. First, although the analytical environment incorporated 52 organizations, 164 cloud environments, 18,764 IoT devices, and 139,684 retained cryptographic assets across multiple sectors and technology categories, the sample could not represent every combination of cloud architecture, IoT platform, hardware configuration, cryptographic library, proprietary protocol, organizational structure, and legacy system currently operating within the United States. Second, cryptographic inventory completeness remained dependent on the visibility provided by configuration data, certificates, system logs, software metadata, firmware information, and dependency records; therefore, undocumented cryptographic components, dynamically loaded libraries, proprietary firmware, shadow assets, and deeply embedded dependencies may have remained undetected. Third, the experimental performance of ML-KEM, ML-DSA, and SLH-DSA was influenced by processor architecture, memory capacity, compiler optimization, cryptographic implementation, virtualization, workload intensity, network conditions, and security parameters, meaning that the reported latency, throughput, memory, bandwidth, and energy values should not be interpreted as universal performance characteristics for every deployment environment. Fourth, simulated and laboratory-controlled IoT conditions could not fully reproduce all operational characteristics of geographically distributed production systems, including unstable connectivity, extreme energy constraints, hardware degradation, intermittent gateway availability, and vendor-specific implementation behavior. Fifth, although XGBoost and other machine-learning models demonstrated strong cross-validation and holdout performance, predictive accuracy depended on the quality, representativeness, and completeness of the input features. Legacy devices and low-visibility environments produced comparatively weaker predictive outcomes, demonstrating that AI could not completely compensate for incomplete telemetry or poorly documented infrastructure. Sixth, migration-priority classifications incorporated measurable technical and organizational variables but could not capture every business, contractual, legal, procurement, operational-continuity, or vendor-related constraint influencing real implementation decisions. Seventh, the evaluation concentrated on NIST-standardized post-quantum algorithms and therefore did not provide an equivalent experimental assessment of every alternative cryptographic mechanism or implementation profile. Eighth, interoperability testing covered major cloud, edge, embedded, and IoT configurations but could not exhaustively reproduce every software version, certificate authority, protocol stack, third-party integration, and vendor ecosystem. Finally, the quantitative design primarily evaluated measurable technical and organizational outcomes and therefore provided limited insight into qualitative factors such as managerial perceptions, organizational resistance, practitioner experience, and internal decision-making processes. These limitations do not invalidate the observed relationships but define the empirical boundaries within which the findings should be interpreted and applied.

REFERENCES

- [1]. Abdullah Mohammad, S. (2023). CUGAO₂ and CUINS₂ Quantum Dot Sensitization for Enhanced Photovoltaic Efficiency in Wearable Fiber-Shaped Solar Cells. *American Journal of Advanced Technology and Engineering Solutions*, 3(04), 209-261. <https://doi.org/10.63125/wysdvy71>
- [2]. Abdullah Mohammad, S. (2026). An AL/ML Integrated Framework for Process Optimization and Advanced Materials Integration in U.S. Oil and Gas Chemical Manufacturing: From Nanostructured Research to Industrial Application. *International Journal of Scientific Interdisciplinary Research*, 7(1), 727-773. <https://doi.org/10.63125/495txr49>
- [3]. Addad, R. A., Dutra, D. L. C., Taleb, T., & Flinck, H. (2021). AI-based network-aware service function chain migration in 5G and beyond networks. *IEEE Transactions on Network and Service Management*, 19(1), 472-484.

- [4]. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71(8), 939-953.
- [5]. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, 11(1), 16.
- [6]. Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating messaging protocols for the Internet of Things (IoT). *Ieee Access*, 8, 94880-94911.
- [7]. Alkhatib, R., & Gaede, K. I. (2024). Data management in biobanking: strategies, challenges, and future directions. *BioTech*, 13(3), 34.
- [8]. Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, 23(17), 7470.
- [9]. Ancarani, A., Di Mauro, C., Legenvre, H., & Cardella, M. S. (2020). Internet of things adoption: a typology of projects. *International Journal of Operations & Production Management*, 40(6), 849-872.
- [10]. Aruna, M., Hasan, M. K., Islam, S., Mohan, K., Sharan, P., & Hassan, R. (2022). Cloud to cloud data migration using self sovereign identity for 5G and beyond. *Cluster computing*, 25(4), 2317-2331.
- [11]. Ashrafuzzaman, M. (2024). The impact of cloud-based management information systems on hrm efficiency: an analysis of small and medium-sized enterprises (SMES). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, 1(01), 40-56. <https://doi.org/10.69593/ajaimldsmis.v1i01.124>
- [12]. Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. 2024 15th International Conference on Network of the Future (NoF),
- [13]. Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal: A Global Perspective*, 29(5), 250-266.
- [14]. Boretti, A. (2024). Technical, economic, and societal risks in the progress of artificial intelligence driven quantum technologies. *Discover artificial intelligence*, 4(1), 67.
- [15]. Bourechak, A., Zedadra, O., Kouahla, M. N., Guerrieri, A., Seridi, H., & Fortino, G. (2023). At the confluence of artificial intelligence and edge computing in iot-based applications: A review and new perspectives. *Sensors*, 23(3), 1639.
- [16]. Budhwar, P., Chowdhury, S., Wood, G., Aguinis, H., Bamber, G. J., Beltran, J. R., Boselie, P., Lee Cooke, F., Decker, S., & DeNisi, A. (2023). Human resource management in the age of generative artificial intelligence: Perspectives and research directions on ChatGPT. *Human Resource Management Journal*, 33(3), 606-659.
- [17]. Bugshan, N., Khalil, I., Moustafa, N., & Rahman, M. S. (2021). Privacy-preserving microservices in industrial internet-of-things-driven smart applications. *IEEE Internet of Things Journal*, 10(4), 2821-2831.
- [18]. Cabrini, F. H., Valiante Filho, F., Rito, P., Barros Filho, A., Sargento, S., Venancio Neto, A., & Kofuji, S. T. (2021). Enabling the industrial Internet of Things to cloud continuum in a real city environment. *Sensors*, 21(22), 7707.
- [19]. Cap, C., Kawaguchi, S., Lupo, J., & Trinidad, C. (2024). Secure communications for quantum and beyond: Orchestrated cryptography for agility and policy. In *Counterterrorism and cybersecurity: total information awareness* (pp. 569-584). Springer.
- [20]. Chéour, R., Khriji, S., & Kanoun, O. (2020). Microcontrollers for IoT: optimizations, computing paradigms, and future directions. 2020 IEEE 6th World Forum on Internet of Things (WF-IoT),
- [21]. Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies*, 12(12), 241.
- [22]. Choi, D., Chung, C. Y., Seyha, T., & Young, J. (2020). Factors affecting organizations' resistance to the adoption of blockchain technology in supply networks. *Sustainability*, 12(21), 8882.
- [23]. Comande, G., & Varilek, M. (2024). The many features which make the eIDAS 2 Digital Wallet either risky or the ideal vehicle for the transition to post-quantum encryption. *Computer Law & Security Review*, 54, 106022.
- [24]. Dayalan, U. K., Fezeu, R. A., Varyani, N., Salo, T. J., & Zhang, Z.-L. (2021). Veeredge: towards an edge-centric iot gateway. 2021 IEEE/ ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid),
- [25]. Debasish, A. (2021). Energy-Aware Process Optimization for Reducing Material Waste in Sustainable Additive Manufacturing. *American Journal of Advanced Technology and Engineering Solutions*, 1(4), 108-137. <https://doi.org/10.63125/j0wk7j48>
- [26]. Debasish, A. (2022). Simulation-Based Thermal Management Framework for Reducing Energy Consumption in Advanced Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, 1(01), 335-381. <https://doi.org/10.63125/6fcj7c89>
- [27]. Debasish, A. (2023). Thermal Behavior Modeling for Predicting Process Instability in Additive Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, 4(4), 485-528. <https://doi.org/10.63125/b2nemb48>
- [28]. Debasish, A. (2024). AI-Based Quality Control Framework for Reducing Rework and Scrap in Additive Manufacturing Production. *Review of Applied Science and Technology*, 3(04), 402-447. <https://doi.org/10.63125/z29tv526>
- [29]. Debasish, A. (2025a). Design-for-Manufacturing Optimization for Improving Resilience in U.S. Additive Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, 6(02), 185-204. <https://doi.org/10.63125/hxm3tb71>
- [30]. Debasish, A. (2025b). Physics-Informed Machine Learning for Predicting Thermal Distortion in Metal Additive Manufacturing. *American Journal of Scholarly Research and Innovation*, 4(01), 943-989. <https://doi.org/10.63125/ny974y17>

- [31]. Dritsas, E., Ramantas, K., & Verikoukis, C. (2024). A mobility-aware reinforcement learning proactive solution for state data migration in edge computing. 2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD),
- [32]. Edwards, D. J. (2024). Inventory and Control of Software Assets. In *Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls* (pp. 29-56). Springer.
- [33]. Freas, R. L., Adair, H. F., & Hammad, E. (2022). An engineering process framework for cybersecurity incident response assessment. 2022 IEEE Conference on Dependable and Secure Computing (DSC),
- [34]. Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462.
- [35]. Hale, B., Bindel, N., & Van Bossuyt, D. L. (2023). Quantum computers: the need for a new cryptographic strategy. In *Handbook for management of threats: security and defense, resilience and optimal strategies* (pp. 125-158). Springer.
- [36]. Hamid, N. A. W. A., & Singh, B. (2024). High-performance computing based operating systems, software dependencies and IoT integration. In *High Performance Computing in Biomimetics: Modeling, Architecture and Applications* (pp. 175-204). Springer.
- [37]. Hasan, K. F., Simpson, L., Bae, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *Ieee Access*, 12, 23427-23450.
- [38]. Herath, T. C., Herath, H. S., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, 25(2), 681-721.
- [39]. Hew, Y., Kutuk, D., Duzcu, T., Ergun, Y., & Basar, M. (2024). Artificial intelligence in IVF laboratories: elevating outcomes through precision and efficiency. *Biology*, 13(12), 988.
- [40]. Hiller, J., Henze, M., Zimmermann, T., Hohlfeld, O., & Wehrle, K. (2019). The case for session sharing: relieving clients from TLS handshake overheads. 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium),
- [41]. How, M.-L., & Cheah, S.-M. (2024). Forging the future: strategic approaches to quantum AI integration for industry transformation. *Ai*, 5(1), 290-323.
- [42]. Jahanara, A. (2025). AI-Enabled Workforce Management: Its Impact on Employee Burnout, Staffing Efficiency, and Organizational Performance in Healthcare. *Review of Applied Science and Technology*, 4(04), 247-295. <https://doi.org/10.63125/5617ff74>
- [43]. Jahanara, A. (2026). Impact of Artificial Intelligence on Operational Efficiency and Cost Reduction in U.S. Healthcare Organizations. *American Journal of Interdisciplinary Studies*, 7(02), 225-276. <https://doi.org/10.63125/3p24ma43>
- [44]. Jang, I., Kim, H., Lee, D., Son, Y.-S., & Kim, S. (2020). Knowledge transfer for on-device deep reinforcement learning in resource constrained edge computing systems. *Ieee Access*, 8, 146588-146597.
- [45]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning-Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2865-2922. <https://doi.org/10.63125/m738bh82>
- [46]. Jannatul, F. (2026). Predicting Falls and Mobility Decline Among Older Adults Using Longitudinal Functional Data and Ensemble Machine Learning. *International Journal of Scientific Interdisciplinary Research*, 7(1), 581-631. <https://doi.org/10.63125/56hans40>
- [47]. Jnr, B. A., Sylva, W., Watat, J. K., & Misra, S. (2024). A framework for standardization of distributed ledger technologies for interoperable data integration and alignment in sustainable smart cities. *Journal of the Knowledge Economy*, 15(3), 12053-12096.
- [48]. Kalogiannidis, S., Kalfas, D., Papaevangelou, O., Giannarakis, G., & Chatzitheodoridis, F. (2024). The role of artificial intelligence technology in predictive risk assessment for business continuity: A case study of Greece. *Risks*, 12(2), 19.
- [49]. Kazi Mohammad Khalid, A. (2026). A Systematic Review of GeoAI and Deep Learning for Automated Road Infrastructure Damage Detection Using Satellite Imagery. *American Journal of Data Science and Analytics*, 7(03), 208-255. <https://doi.org/10.63125/77cy0h19>
- [50]. Kazi Rakib Hasan, S., & Adnan, S. (2022). Quantitative Assessment of Machine Learning-Based Schedule Risk Prediction for Reducing Delays in Complex Technology Projects. *Review of Applied Science and Technology*, 1(04), 464-501. <https://doi.org/10.63125/dn8nkm85>
- [51]. Kendzierskyj, S., Jahankhani, H., & Hussien, O. A. A. M. (2024). Space governance frameworks and the role of AI and quantum computing. In *Space Governance: Challenges, Threats and Countermeasures* (pp. 1-39). Springer.
- [52]. Khan, M. A., Hamila, R., Erbad, A., & Gabbouj, M. (2022). Distributed inference in resource-constrained IoT for real-time video surveillance. *IEEE Systems Journal*, 17(1), 1512-1523.
- [53]. Khang, A., & Rath, K. C. (2024). The quantum evolution. *Application of AI and Robotics in the Future of Quantum Technology*.
- [54]. Kim, B., Mun, H.-G., Lee, K.-J., Woo, J.-M., Kang, K., Son, H., & Sim, J.-Y. (2024). A 243 KOPS/W crypto-processor supporting homomorphic encryption and post-quantum cryptography for IoT devices. 2024 IEEE European Solid-State Electronics Research Conference (ESSERC),
- [55]. Kolimago, C., Robson, M., Olufowobi, H., & Nwafor, E. (2024). Simulating load sharing for resource constrained devices. *Ieee Access*, 12, 157021-157038.
- [56]. Kumar, A., Bhatia, S., Kaushik, K., Gandhi, S. M., Devi, S. G., Pacheco, D. A. D. J., & Mashat, A. (2021). Survey of promising technologies for quantum drones and networks. *Ieee Access*, 9, 125868-125911.

- [57]. Kumar, A. S., & Joshi, P. (2024). Future-proofing industrial protocol security: Integration of post-quantum cryptography in the modbus protocol. *International Conference on Innovations in Cybersecurity and Data Science Proceedings of ICICDS*,
- [58]. Kumar, D. D., Mukharzee, J. D., Reddy, C. V. D., & Rajagopal, S. M. (2024). Safe and secure communication using SSL/TLS. *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)*,
- [59]. Langiu, A., Boano, C. A., Schuß, M., & Römer, K. (2019). Upkit: An open-source, portable, and lightweight update framework for constrained iot devices. *2019 IEEE 39th international conference on distributed computing systems (ICDCS)*,
- [60]. Lin, K., Li, Y., Zhang, Q., & Fortino, G. (2021). AI-driven collaborative resource allocation for task execution in 6G-enabled massive IoT. *IEEE Internet of Things Journal*, 8(7), 5264-5273.
- [61]. Mahbulul, I., Mahmudul, I., Shifa, T., Mahfuza, T., & Shima Ali, S. (2022). Exploring The Potential of Visual Narratives and Interactive Gamified Communication Systems to Prevent Disease, Counter Health Misinformation, And Strengthen Public Trust in Low-Literacy Communities: A Literature Review. *American Journal of Interdisciplinary Studies*, 3(02), 165-220. <https://doi.org/10.63125/zmq4n64>
- [62]. Mahfoudhi, F., Sultania, A. K., & Famaey, J. (2022). Over-the-air firmware updates for constrained NB-IoT devices. *Sensors*, 22(19), 7572.
- [63]. Mahfuj Ahmed, R. (2026). AI-Assisted Credit Evaluation Models for Improving Risk Assessment Accuracy in U.S. Banking Systems. *American Journal of Interdisciplinary Studies*, 7(01), 387-425. <https://doi.org/10.63125/aa031j21>
- [64]. Maitra, S., Richards, D., Abdelgawad, A., & Yelamarthi, K. (2019). Performance evaluation of IoT encryption algorithms: Memory, timing, and energy. *2019 IEEE sensors applications symposium (SAS)*,
- [65]. Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. *Applied Sciences*, 12(21), 11174.
- [66]. Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things*, 27, 101228.
- [67]. Md Anisur Rahman, M. (2024). State Income Tax Differentials and High-Skilled Labor Mobility in The United States: A Time Series Analysis. *American Journal of Interdisciplinary Studies*, 5(04), 222-267. <https://doi.org/10.63125/295bsn47>
- [68]. Md Anisur Rahman, M. (2025). The Role of AI-Enabled Business Intelligence in Financial Risk Assessment and Liquidity Monitoring. *Review of Applied Science and Technology*, 4(04), 195-246. <https://doi.org/10.63125/p4eezd93>
- [69]. Md Anisur Rahman, M. (2026). AI-Driven Business Intelligence for Real-Time Fraud Risk Monitoring in Digital Payment Platforms: A Framework-Based Review. *International Journal of Scientific Interdisciplinary Research*, 7(1), 527-580. <https://doi.org/10.63125/0ef34271>
- [70]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use he Innovative Open And Distance Learning Systems With The Role Of Continuance Intention. *American Journal of Scholarly Research and Innovation*, 4(01), 202-220. <https://doi.org/10.63125/pbjxp014>
- [71]. Md Ashfaq, S., & Abdullah Mohammad, S. (2022). CNT/PANI Composite Electrodes for Flexible Fiber-Shaped Dye-Sensitized Solar Cells: Synthesis, Characterization, and Photovoltaic Performance. *American Journal of Interdisciplinary Studies*, 3(02), 221-274. <https://doi.org/10.63125/m334mf41>
- [72]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807-841. <https://doi.org/10.63125/gm63q956>
- [73]. Md Asif Ali Sheak, A., & Tahmedur, R. (2023). A Data-Driven Framework for Engineering Project Risk Assessment Under Schedule and Cost Uncertainty. *International Journal of Scientific Interdisciplinary Research*, 4(2), 204-251. <https://doi.org/10.63125/kq4zzh16>
- [74]. Md Kaium, H. (2023). A GIS-Based Multi-Criteria Decision-Support and Land-Suitability Optimization Framework for Climate-Resilient Urban and Regional Planning. *American Journal of Data Science and Analytics*, 4(06), 43-103. <https://doi.org/10.63125/wvq0sx87>
- [75]. Md Kaium, H. (2024). Machine Learning Enhanced GIS And AHP Modeling for High-Resolution Flood-Susceptibility Prediction, Vulnerability Assessment, and Risk Classification. *Review of Applied Science and Technology*, 3(02), 92-140. <https://doi.org/10.63125/fz8hv245>
- [76]. Md Kaium, H. (2025). Integrating Artificial Intelligence, Semantic Indoor Geospatial Modeling, And Network-Based Routing for High-Precision NG911 Emergency Location Intelligence. *International Journal of Scientific Interdisciplinary Research*, 6(1), 616-670. <https://doi.org/10.63125/5hc1xx56>
- [77]. Md Kaium, H. (2026). An Artificial Intelligence Integrated Geospatial Decision-Support Framework for Scenario-Based Climate-Adaptive Land-Use Optimization and Environmental Risk Reduction. *American Journal of Data Science and Analytics*, 7(06), 425-483. <https://doi.org/10.63125/nyc7sh45>
- [78]. Md Mahamud Pervaz, P. (2023). Integration of MES, SAP, And PI Historian Platforms for Real-Time Industrial Asset Performance Management. *Review of Applied Science and Technology*, 2(04), 393-445. <https://doi.org/10.63125/9ebtas97>
- [79]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, 4(01), 894-942. <https://doi.org/10.63125/j33gtf31>
- [80]. Md Mahamud Pervaz, P. (2026). Implementation of an OSHA-Compliant Lockout/Tagout and Arc-Flash Hazard Mitigation Framework for U.S. Industrial Maintenance Operations. *American Journal of Interdisciplinary Studies*, 7(02), 73-119. <https://doi.org/10.63125/8ky04n07>

- [81]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70-102. <https://doi.org/10.63125/dyrpc387>
- [82]. Md. Rashedul, I., & Md Kaium, H. (2022). Development Of a Three-Dimensional Indoor Geospatial Network and Address Geocoding Framework for Next-Generation Emergency Dispatch and Response-Time Optimization. *Journal of Sustainable Development and Policy*, 1(02), 245-292. <https://doi.org/10.63125/tcw3mp48>
- [83]. Md. Shakhawat, H., & Md, F. (2024). Impact of Phishing Simulation Campaigns and Security Awareness Training on Human Risk Mitigation in Financial Institutions: A Quantitative Study. *American Journal of Data Science and Analytics*, 5(10), 48-85. <https://doi.org/10.63125/4j8h1484>
- [84]. Medina, F., Molteni, M. C., Di Scala, A. J., & Nava, L. (2024). Analysis and contributions to an open source Kyber library in Rust. 2024 IEEE Symposium on Computers and Communications (ISCC),
- [85]. Michail-Alexandros, K., George, X., Ioannis, C., & Anastasios, K. (2023). Quantum computing and lawful interception applications. *International Conference on Information Technology & Systems*,
- [86]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529-576. <https://doi.org/10.63125/qd6nn437>
- [87]. Mohammad Abir Chowdhury, S. (2025). Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in U.S. Government Financial Operations. *American Journal of Interdisciplinary Studies*, 6(02), 139-184. <https://doi.org/10.63125/fkf19309>
- [88]. Mohammad Abir Chowdhury, S. (2026). Development Of a Machine-Learning Approach for Internal-Control Weakness Prediction and Audit-Risk Scoring In U.S. State Government Agencies. *American Journal of Data Science and Analytics*, 7(06), 380-424. <https://doi.org/10.63125/3v722074>
- [89]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73-126. <https://doi.org/10.63125/7p8dcr47>
- [90]. Mohammad Badrul, A. (2025). SCADA And IOT-Enabled Smart Water Metering: A Systematic Review of Resilient Supply Monitoring. *International Journal of Scientific Interdisciplinary Research*, 6(1), 576-615. <https://doi.org/10.63125/at8pnx81>
- [91]. Mohammad Badrul, A. (2026). A Machine-Learning Framework for Real-Time Non-Revenue Water Prediction in Aging Urban Distribution Networks. *American Journal of Interdisciplinary Studies*, 7(02), 01-52. <https://doi.org/10.63125/93km2h66>
- [92]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning-Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33-77. <https://doi.org/10.63125/y3yfxa92>
- [93]. Mohammad Shoriful Hossan, S. (2022). A Performance-Based Framework for Arc-Flash Hazard Reduction and Electrical Reliability Improvement in Brownfield Industrial Distribution Systems. *Review of Applied Science and Technology*, 1(04), 447-463. <https://doi.org/10.63125/a70vj720>
- [94]. Molla Al Rakib, H., & Mohammad Towhidul, I. (2023). Cyber-Resilient Marketing Intelligence Systems for Fraud Detection and Data Integrity in Digital Campaigns. *American Journal of Scholarly Research and Innovation*, 2(02), 485-518. <https://doi.org/10.63125/b53pgr11>
- [95]. Mst Kaniz, F. (2022). Language Access and Health Equity: Role of Multilingual Administrative Staff in Reducing Healthcare Disparities Among South Asian Immigrant Communities in The U.S. *International Journal of Scientific Interdisciplinary Research*, 1(01), 274-315. <https://doi.org/10.63125/xqhss825>
- [96]. Mst Shamima, A. (2026). Enhancing Financial Accountability and Cost Control in North American Outpatient Clinics Through Data Science: A Mixed-Methods Healthcare Administration Study. *American Journal of Data Science and Analytics*, 7(05), 01-41. <https://doi.org/10.63125/wksqy749>
- [97]. Mukut Kanti, B. (2024). AI-Enabled Predictive Asset Integrity Monitoring for Industrial Equipment in Oil & Gas and Energy Sector Facilities. *International Journal of Scientific Interdisciplinary Research*, 5(2), 746-791. <https://doi.org/10.63125/3mjcah04>
- [98]. Mukut Kanti, B. (2026). Digital-Twin And IOT-Based Condition Monitoring for Rotating Machinery and Process Equipment in Petrochemical and Industrial Environments. *American Journal of Scholarly Research and Innovation*, 5(01), 382-428. <https://doi.org/10.63125/mwdnjv55>
- [99]. Murad, M. D. H. R. (2026). Artificial Intelligence-Driven Enterprise Decision Support Systems: A Framework for Intelligent Business Process Automation in Digital Economies. *American Journal of Advanced Technology and Engineering Solutions*, 6(01), 332-373. <https://doi.org/10.63125/nnv83884>
- [100]. Nanos, I., Manthou, V., & Androutsou, E. (2018). Cloud computing adoption decision in E-government. *Operational Research in the Digital Era-ICT Challenges: 6th International Symposium and 28th National Conference on Operational Research*, Thessaloniki, Greece, June 2017,
- [101]. Nasir, M., Muhammad, K., Ullah, A., Ahmad, J., Baik, S. W., & Sajjad, M. (2022). Enabling automation and edge intelligence over resource constraint IoT devices for smart home. *Neurocomputing*, 491, 494-506.
- [102]. Nishat, J. (2023). Communicable Disease Prevention in a Post-Pandemic Era: A Global Review of Public Health Education, Surveillance, and Community-Level Interventions. *International Journal of Scientific Interdisciplinary Research*, 4(4), 630-678. <https://doi.org/10.63125/mnqefj36>
- [103]. Nishat, J. (2025). Leveraging Machine Learning to Identify and Address Maternal Health Disparities in Underserved U.S. Communities. *American Journal of Data Science and Analytics*, 6(12), 125-169. <https://doi.org/10.63125/c2t7r719>

- [104]. Nishat, J. (2026). Predictive Analytics for Program Effectiveness: A Machine Learning Approach to Health Education Programs in the United States. *American Journal of Health and Medical Sciences*, 7(03), 30-56. <https://doi.org/10.63125/2vw42878>
- [105]. Nishat, J., & Jahanara, A. (2024). Machine Learning Approaches for Early Prediction of High-Risk Pregnancy in Underserved U.S. Populations. *American Journal of Interdisciplinary Studies*, 5(04), 268-309. <https://doi.org/10.63125/5gh5df13>
- [106]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223-269. <https://doi.org/10.63125/vgv5s742>
- [107]. Nuzhat Sadia, P. (2025). Integrating Business Intelligence Dashboards for Real-Time Supply Chain Visibility and Operational Decision Support. *American Journal of Data Science and Analytics*, 6(12), 170-216. <https://doi.org/10.63125/1es4f763>
- [108]. Nuzhat Sadia, P. (2026). An Integrated IT Management Framework for Scenario-Based Enterprise Analytics and Strategic Decision Optimization. *American Journal of Interdisciplinary Studies*, 7(02), 120-168. <https://doi.org/10.63125/3wtc3z49>
- [109]. Okay, F. Y., & Ozdemir, S. (2018). Routing in fog-enabled IoT platforms: A survey and an SDN-based solution. *IEEE Internet of Things Journal*, 5(6), 4871-4889.
- [110]. Pei Breivold, H. (2020). Towards factories of the future: migration of industrial legacy automation systems in the cloud computing and Internet-of-things context. *Enterprise Information Systems*, 14(4), 542-562.
- [111]. Petrenko, K., Mashatan, A., & Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. *Journal of Information Security and Applications*, 46, 151-163.
- [112]. Protzenko, J., Parno, B., Fromherz, A., Hawblitzel, C., Polubelova, M., Bhargavan, K., Beurdouche, B., Choi, J., Delignat-Lavaud, A., & Fournet, C. (2020). Evercrypt: A fast, verified, cross-platform cryptographic provider. 2020 IEEE Symposium on Security and Privacy (SP),
- [113]. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., Maddox, L. T., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, 3(1), 13.
- [114]. Rony, S., & Md, A. (2026). Multi-Agency Coordination in Sustained Healthcare Supply Shortages: Lessons from Covid-19, Drug Shortages, and Critical Medical Supply Disruptions. *American Journal of Data Science and Analytics*, 7(01), 181-221. <https://doi.org/10.63125/5v6t8515>
- [115]. Rukaiya Khatun, M. (2026). Machine Learning-Based Transaction Risk Scoring Models for Financial Compliance Monitoring in Foreign Exchange Operations. *International Journal of Scientific Interdisciplinary Research*, 7(1), 172-203. <https://doi.org/10.63125/0nbg6w69>
- [116]. Saarinen, M.-J. O. (2024). Accelerating SLH-DNA by two orders of magnitude with a single hash unit. Annual International Cryptology Conference,
- [117]. Saceleanu, V. M., Toader, C., Ples, H., Covache-Busuioc, R.-A., Costin, H. P., Bratu, B.-G., Dumitrascu, D.-I., Bordeianu, A., Corlatescu, A. D., & Ciurea, A. V. (2023). Integrative approaches in acute ischemic stroke: from symptom recognition to future innovations. *Biomedicine*, 11(10), 2617.
- [118]. Sadia, Z. (2025). Predictive Analytics for Financial Performance Forecasting and Reporting Quality: Evidence from Data-Driven Financial Management Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2795-2812. <https://doi.org/10.63125/zstqn346>
- [119]. SasiKumar, S., Sundar, K., Jayakumar, C., Obaidat, M. S., Stephan, T., & Hsiao, K.-F. (2022). Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment. *Simulation Modelling Practice and Theory*, 121, 102651.
- [120]. Senevirathna, T., La, V. H., Marcha, S., Siniarski, B., Liyanage, M., & Wang, S. (2024). A survey on XAI for 5G and beyond security: Technical aspects, challenges and research directions. *IEEE Communications Surveys & Tutorials*, 27(2), 941-973.
- [121]. Sepulveda, S., Cravero, A., Fonseca, G., & Antonelli, L. (2024). Systematic review on requirements engineering in quantum computing: Insights and future directions. *Electronics*, 13(15), 2989.
- [122]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [123]. Shamsul, A. (2026). Electrical Engineering Approaches for AI-Enabled Autonomous Robotics in U.S. Industrial and Defense Applications. *International Journal of Scientific Interdisciplinary Research*, 7(1), 72-110. <https://doi.org/10.63125/h255cq52>
- [124]. Sharma, G., Hemrajani, N., Sharma, S., Upadhyay, A., Bhardwaj, Y., & Kumar, A. (2022). Data management framework for IoT edge-cloud architecture for resource-constrained IoT application. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1093-1103.
- [125]. Shuvo, M. M. H., Islam, S. K., Cheng, J., & Morshed, B. I. (2022). Efficient acceleration of deep learning inference on resource-constrained edge devices: A review. *Proceedings of the IEEE*, 111(1), 42-91.
- [126]. Shyam, R., Swetha, C., & Jesupriya, J. Quantum threats and federated AI. In *Federated Learning in Finance* (pp. 215-234). CRC Press.

- [127]. Silonosov, A., & Henesey, L. (2024). Towards cryptographic agility manifesto in end-to-end encryption systems: A position paper from the perspective of crypto-consumers. 2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC),
- [128]. Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects. *IEEE Communications Surveys & Tutorials*, 23(2), 1160-1192.
- [129]. Sowa, J., Hoang, B., Yeluru, A., Qie, S., Nikolich, A., Iyer, R., & Cao, P. (2024). Post-quantum cryptography (pqc) network instrument: Measuring pqc adoption rates and identifying migration pathways. 2024 IEEE International Conference on Quantum Computing and Engineering (QCE),
- [130]. Straut, C. M., & Nelson, A. (2020). Improving chemical security with material control and accountability and inventory management. *Journal of chemical education*, 97(7), 1809-1814.
- [131]. Töbke, L., Grote, O., & Ahrens, A. (2023). A Practical Approach to Quantum Resilient Cloud Usage Obtaining Data Privacy. 2023 International Interdisciplinary PhD Workshop (IIPhDW),
- [132]. Tonay, P. (2025). Machine Learning for Fraud Detection in Enterprise Financial Systems. *American Journal of Advanced Technology and Engineering Solutions*, 1(02), 304-318. <https://doi.org/10.63125/d0fhp873>
- [133]. Tonay, P. (2026). The Role of AI-Based Decision Support in Financial Risk Management and Anomaly Detection. *American Journal of Data Science and Analytics*, 7(06), 327-359. <https://doi.org/10.63125/wnb54w77>
- [134]. Tonay, P., Md Maruf, I., & Al, A. (2024). Artificial Intelligence-Based Decision Support Systems and Managerial Performance. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 154-184. <https://doi.org/10.63125/wmz8dc67>
- [135]. Touni, N., Bagaa, M., & Ksentini, A. (2023). Machine learning for service migration: A survey. *IEEE Communications Surveys & Tutorials*, 25(3), 1991-2020.
- [136]. Uddin, H. M. M., & Risha, A. (2024). Hybrid Cloud Security and Compliance in U.S. Enterprises: Addressing Data Privacy Risks and Governance Challenges. *American Journal of Scholarly Research and Innovation*, 3(01), 153-197. <https://doi.org/10.63125/qcy0cj46>
- [137]. Vance, D., Jin, M., Price, C., Nimbalkar, S. U., & Wenning, T. (2023). Smart manufacturing maturity models and their applicability: a review. *Journal of Manufacturing Technology Management*, 34(5), 735-770.
- [138]. Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., Soos, G., Ficzer, D., Maliosz, M., & Toka, L. (2020). 5G support for industrial IoT applications – challenges, solutions, and research gaps. *Sensors*, 20(3), 828.
- [139]. Ye, X., Tan, T. G., & Zhou, J. (2024). Towards Discovering Quantum-Threats for Applications Using Open-Source Libraries. International Conference on Applied Cryptography and Network Security,
- [140]. Yenugula, M. (2024). AI Based Workflow Scheduling and Automatic Migration Planning Model for Cloud Computing. International Conference on Advanced Computing and Applications,
- [141]. Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained iot devices using open standards: A reality check. *Ieee Access*, 7, 71907-71920.
- [142]. Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A., & Luzcando, E. (2022). Practical adoption of cloud computing in power systems – Drivers, challenges, guidance, and real-world use cases. *IEEE Transactions on Smart Grid*, 13(3), 2390-2411.