American Journal of Interdisciplinary Studies

Volume: 2; **Issue:** 4
Pages: 101-134
eISSN: 3067-5146

POST-QUANTUM CRYPTOGRAPHY FRAMEWORKS FOR SECURING GLOBAL CLOUD SYSTEMS

Sai Srinivas Matta[1]; Manish Bolli[2];

[1]. MS in CS Candidate, Campbellsville University, USA; Email: mattasaisrinivas@gmail.com
[2]. MS in CS Candidate, University of Central Missouri, Email : manishbolli66@gmail.com

Doi: 10.63125/dhbvry98
Received: *29 September 2021;* ***Revised:*** *28 October 2021;* ***Accepted:*** *19 November 2021;* ***Published:*** *28 December 2021*

Abstract

This study addresses the emerging problem that quantum attacks can undermine classical public key cryptography that secures global cloud platforms, leaving long lived, cross border data at risk, and evaluates how far organizations have progressed toward post quantum cryptography (PQC) frameworks. The purpose is to quantify PQC framework maturity and its security, compliance, and performance implications in cloud and enterprise cases. Using a quantitative, cross sectional, case-based design, survey data were collected from 220 organizations that provide or consume multi region cloud services, with key informants in security, cloud architecture, and compliance rating Likert five-point items. Core variables included PQC awareness, adoption intention, regulatory and contractual pressure, security governance capability, perceived performance impact, PQC framework maturity, perceived quantum resilient security posture, perceived regulatory compliance, and perceived operational performance. Descriptive statistics, reliability and validity tests, Pearson correlations, and multiple regression models with sector, size, region, and deployment model as controls were applied. Results show moderate PQC maturity (mean 3.21) but higher awareness (3.68) and adoption intention (3.55). PQC maturity correlated strongly with quantum resilient security posture ($r = 0.68$) and regulatory compliance ($r = 0.64$), and significantly predicted both outcomes ($\beta = 0.59$ and $\beta = 0.55$, $R^2 = 0.47$ and 0.42). Regulatory pressure ($\beta = 0.34$) and governance capability ($\beta = 0.18$) were also significant drivers of maturity. These findings imply that building systematic, governance anchored PQC frameworks can measurably strengthen cloud security and compliance while maintaining acceptable performance, guiding prioritized, phased PQC migration for global cloud providers and enterprise users.

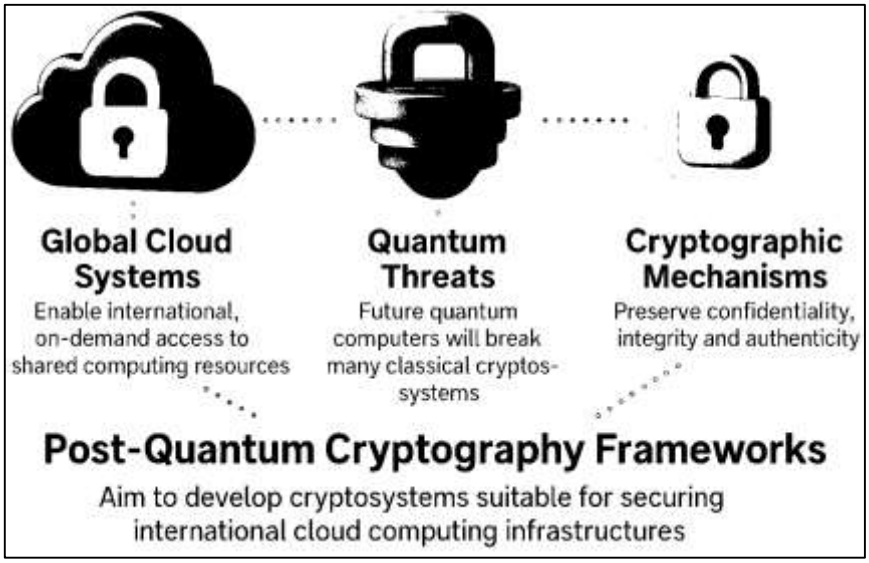
Keywords

Post Quantum Cryptography; Global Cloud Systems; Cryptographic Framework Maturity; Quantum Resilient Security; Cloud Compliance;

INTRODUCTION

Post-quantum cryptography frameworks for securing global cloud systems sit at the intersection of two international infrastructures: the worldwide cloud computing ecosystem and the cryptographic mechanisms that preserve confidentiality, integrity, and authenticity of digital assets. Cloud computing enables elastic, on-demand access to shared pools of configurable resources across borders and jurisdictions, supporting critical services in government, healthcare, finance, and industry (Zhang et al., 2010). In this model, data and workloads routinely traverse data centers in multiple countries, making security controls inseparable from questions of sovereignty, compliance, and service-level assurance (Zissis & Lekkas, 2012). Researchers have shown that multitenancy, virtualization layers, and service-delivery models introduce compound attack surfaces that extend beyond traditional perimeter-based security (Hashizume et al., 2013). Survey and analytical work on cloud security emphasizes that data protection, identity and access management, and secure virtualization are among the central concerns for large-scale cloud deployments, particularly when providers operate globally distributed infrastructures (Bisong & Rahman, 2011). At the same time, studies on data security and privacy in cloud computing underline that customer data are frequently stored and processed in geographically dispersed locations, which intensifies worries about unauthorized access, data breaches, and regulatory non-compliance (Jin et al., 2014). Within this international context, cryptography functions as a foundational control for safeguarding data in transit, at rest, and in use, yet the cryptographic primitives underlying many existing cloud security controls are tightly linked to hardness assumptions that quantum computing challenges (Bernstein, 2009).

Figure 1: Key Components of Post-Quantum Cryptography in International Cloud Security



Classical public-key cryptography that underpins secure communication channels, key management systems, and digital signatures in cloud platforms predominantly relies on number-theoretic problems such as integer factorization and discrete logarithms. These problems form the security basis for widely deployed schemes such as RSA, DSA, and elliptic-curve cryptography and are embedded in protocols like TLS, IPsec, and S/MIME that cloud providers use for client–server and service–service communication (Cayrel & Meziani, 2010). Analytical treatments of quantum algorithms have demonstrated that large, fault-tolerant quantum computers can solve these underlying problems in polynomial time, which in turn breaks the security guarantees of many current public-key systems (Yan, 2013). This body of work portrays a cryptographic landscape in which the existence of scalable quantum computers is formally linked to efficient attacks against core cryptosystems, transforming theoretical advances into concrete security concerns for infrastructures that depend on long-term confidentiality, such as archival cloud storage and key escrow services (Mosca, 2018). Strategic analyses in cybersecurity research characterize this situation as a cryptographic transition problem, where organizations relying on long-lived data must consider the risk that encrypted information harvested

in the present can be decrypted once quantum capabilities reach relevant thresholds (Micciancio & Regev, 2009). For global cloud systems that manage sensitive records, financial transactions, and industrial telemetry, this transition problem is tightly coupled with cross-border data flows and international regulatory environments, which frequently prescribe retention periods and auditability requirements that exceed the anticipated lifetime of current public-key schemes (Overbeck & Sendrier, 2009).

Post-quantum cryptography (PQC) has emerged as a prominent response to these quantum threats, aiming to provide cryptographic schemes that remain secure under adversaries equipped with large quantum computers while retaining the operational properties of classical public-key systems. PQC is commonly defined as the development of public-key encryption, key establishment, and digital signature algorithms whose security rests on problems believed to resist both classical and quantum attacks, while remaining implementable on conventional computing platforms. Comprehensive treatments of PQC classify candidate systems into several main families, including lattice-based, code-based, multivariate-quadratic, and hash-based schemes, each grounded in distinct hardness assumptions and algebraic structures (Cayrel & Meziani, 2010). Within this taxonomy, researchers highlight not only asymptotic security but also implementation considerations such as key sizes, computational overhead, and side-channel resistance, which are crucial for integration into high-throughput environments like multi-tenant clouds (Subashini & Kavitha, 2011). Survey and tutorial works in PQC underline that many of these schemes can be instantiated using existing software and hardware primitives, making them candidates for incremental deployment in Internet-scale systems where classical and quantum-resistant protocols may coexist for extended periods (Naehrig et al., 2011). For globally distributed cloud platforms, these characteristics frame PQC simultaneously as a mathematical subject and as a practical design space for constructing key management and data-protection frameworks that align with the elasticity and heterogeneity of cloud services (Carlin & Curran, 2011).

Among the candidate PQC families, lattice-based cryptography has attracted substantial attention for its combination of strong security reductions and favorable efficiency properties. The learning with errors (LWE) problem and its variants are central to this line of work, with reductions from worst-case lattice problems to average-case instances of LWE providing a rigorous foundation for constructing cryptosystems whose security can be related to well-studied approximation problems on lattices (Gentry, 2009). Building on these results, overviews of lattice-based cryptography survey encryption, signature, and identification schemes derived from lattice problems, emphasizing conceptual simplicity, parallelizability, and conjectured resistance to quantum algorithms (Khalil et al., 2014). The construction of fully homomorphic encryption over ideal lattices illustrated that lattice-based schemes can support arbitrary computation over encrypted data, a property that fits naturally with outsourced computation scenarios common in cloud platforms (Regev, 2009). Subsequent work examined the practicality of such homomorphic schemes, analyzing parameter choices and performance trade-offs to determine feasible deployment profiles in real systems (Ara, 2021; Jahid, 2021; Naehrig et al., 2011). In parallel, research on lattice-based digital signatures has produced schemes tailored for constrained devices and embedded environments, including constructions focused on key and signature size reductions suitable for large-scale deployment (Howe et al., 2015; Akbar & Farzana, 2021; Reza et al., 2021). These contributions portray lattice-based PQC as a versatile foundation for encryption, key encapsulation, and signatures that can be aligned with the performance and scalability demands of global cloud infrastructures (Gentry, 2009; Saikat, 2021; Shaikh & Aditya, 2021).

Code-based and multivariate post-quantum schemes provide complementary design options that broaden the range of frameworks available for securing cloud systems. Code-based cryptography is rooted in the hardness of decoding general linear codes, and modern expositions focus on optimized constructions and parameter choices that reduce key sizes and improve efficiency while maintaining security margins (Overbeck & Sendrier, 2009; Kanti & Shaikat, 2021). Within this line of work, code-based signature schemes, including threshold and ring variants, demonstrate how distributed trust and flexible authorization models can be built using code-based primitives (Cayrel & Meziani, 2010). Multivariate-quadratic systems, based on solving systems of polynomial equations over finite fields, are also studied as candidates for post-quantum public-key primitives, with investigations into their

algebraic structures and resistance to known cryptanalytic techniques (Regev, 2009). These families exhibit different trade-offs from lattice-based constructions, particularly regarding key sizes, signature lengths, and implementation complexity (Micciancio & Regev, 2009). From the standpoint of cloud security frameworks, the existence of diverse PQC families allows system architects to consider heterogeneous portfolios of algorithms mapped to specific use cases, such as high-throughput internal service authentication, long-term archival encryption, or lightweight client-side operations in edge–cloud configurations (Bernstein, 2009). Analyses of quantum attacks on public-key systems reinforce the rationale for such diversification by documenting the range of quantum algorithms and their impact on various classes of hardness assumptions (Yan, 2013). These insights shape discussions of how post-quantum frameworks for global clouds can combine multiple algorithmic families to align security and performance requirements across layers of the cloud stack (Bernstein, 2009).

Research on cloud security provides complementary perspectives on how cryptographic mechanisms, including PQC, must be embedded into broader architectural and governance frameworks to address the distinctive risks of cloud environments. Cloud computing has been described as a service-oriented paradigm with layered abstractions—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—each associated with specific threat profiles and control responsibilities (Zhang et al., 2010). Security challenges across these service-delivery models include data segregation, access control, and secure virtualization as key areas where cryptographic controls must integrate with platform mechanisms (Subashini & Kavitha, 2011). Analyses of security issues for cloud computing identify vulnerabilities that arise from outsourcing essential services to third-party providers, with implications for data confidentiality, availability, and regulatory compliance (Hashizume et al., 2013). Reference security architectures for the cloud often combine encryption, identity management, and trust evaluation to safeguard cloud services, emphasizing the necessity of systematic frameworks rather than ad hoc control deployment (Zissis & Lekkas, 2012). Empirical studies focused on enterprise cloud adoption indicate that organizations evaluate security in terms of risk, cost, and control over assets, with cryptographic mechanisms regarded as one among several interdependent safeguards that also include network segmentation, logging, and incident response (González et al., 2016). These strands of research collectively show that a post-quantum framework for securing global cloud systems must be considered within a larger fabric of security requirements, architectural patterns, and organizational expectations (Howe et al., 2015).

Specialist studies on data security and privacy in cloud computing draw additional attention to the regulatory and jurisdictional dimensions that shape how cryptographic frameworks are selected and implemented. Data security and privacy protection in cloud computing are central to user trust, particularly in environments where data may reside in multiple legal contexts and be subject to varied disclosure obligations (Arfan et al., 2021; González et al., 2016). Work on modeling and ontologies for cloud security illustrates how stakeholders conceptualize security properties, assets, and threats, and shows that differing interpretations of these concepts can slow cloud adoption when organizations struggle to map high-level requirements to concrete controls (Khalil et al., 2014). Risk-oriented surveys highlight that quantitative models for assessing security in cloud environments often treat cryptography as a parameter within larger risk equations that include service availability, likelihood of incidents, and impact on business processes (González et al., 2016). These perspectives frame PQC as a component of governance arrangements that must account for auditability, key lifecycle management, incident response, and alignment with standards and regulations in multiple jurisdictions (Jin et al., 2014). For global cloud systems subject to data protection laws, sectoral regulations, and international standards, the choice and configuration of post-quantum algorithms intersect with compliance obligations, certification schemes, and contractual agreements between providers and customers (González et al., 2016).

Against this backdrop, research on post-quantum cryptography frameworks for securing global cloud systems can draw simultaneously on cryptographic theory, cloud security architecture, and empirical analyses of organizational behavior. Cryptographic studies characterize the security and performance properties of lattice-based, code-based, and related post-quantum schemes (Bernstein, 2009), while cloud security work maps the threat landscape and architectural responses in multi-tenant environments (Bisong & Rahman, 2011). Empirical perspectives on cloud risk and data protection

further describe how regulatory, organizational, and technical factors jointly shape security decision-making (González et al., 2016). Within this combined literature, quantitative, cross-sectional, case-study–based investigations can employ Likert-type scales to operationalize constructs such as perceived security enhancement, integration complexity, performance impact, and regulatory alignment in the context of PQC deployment within cloud architectures. Studies targeting organizations that consume or provide cloud services across national boundaries can examine how technical parameters of PQC schemes interact with organizational policies, compliance requirements, and existing security architectures (Carlin & Curran, 2011). By applying descriptive statistics, correlation analysis, and regression modeling to such data, research can quantify relationships among cryptographic choices, architectural patterns, and organizational drivers, offering an empirically grounded view of how post-quantum cryptographic frameworks are understood and positioned within international cloud infrastructures (González et al., 2016).

This study is undertaken with the primary objective of systematically examining how post-quantum cryptography frameworks can be designed, evaluated, and integrated to enhance the security of global cloud systems within real organizational environments. The research first aims to assess the current level of awareness, preparedness, and practical engagement with quantum-resistant cryptographic solutions among organizations that provide or consume cloud services across multiple jurisdictions. In doing so, it seeks to capture how decision makers, security architects, and technical practitioners understand quantum-related risks and how they position post-quantum mechanisms within their broader cloud security strategies. A second objective is to identify and quantify the organizational, technical, and regulatory factors that shape the adoption and maturity of post-quantum frameworks in cloud infrastructures. This includes examining perceived benefits, perceived performance impact, integration complexity, cost considerations, skills availability, and alignment with legal and compliance requirements. A third objective is to develop a structured set of measurable constructs that represent key dimensions of post-quantum cloud security, such as framework maturity, perceived security enhancement, perceived compliance support, and operational fit, and to validate these constructs through a quantitative survey-based instrument. A fourth objective is to use descriptive statistics, correlation analysis, and regression modeling to analyze relationships among these constructs, thereby identifying which factors most strongly influence the progression from awareness and intention to concrete implementation of post-quantum frameworks in cloud architectures. A fifth objective is to derive, from the empirical patterns observed in the participating organizations, a practical, layered framework that links specific types of post-quantum algorithms and controls to particular cloud service models and deployment scenarios, such as public, private, hybrid, and multi-cloud configurations. Finally, the study seeks to articulate, in a structured and evidence-informed manner, how organizations at different stages of readiness can move from existing cryptographic baselines to more mature post-quantum security postures, using clear constructs, measurable indicators, and analytically supported relationships as the foundation for subsequent methodological, architectural, and governance decisions in global cloud environments.

LITERATURE REVIEW

The literature on post-quantum cryptography and cloud security spans several intersecting domains, including fundamental cryptographic theory, post-quantum algorithm design, cloud computing architectures, and empirical studies of security management in distributed environments. Foundational work in post-quantum cryptography introduces quantum-resistant public-key primitives—such as lattice-based, code-based, multivariate, and hash-based schemes—as candidates to replace or augment traditional number-theoretic algorithms that underlie today's Internet and cloud security protocols, particularly those vulnerable to Shor-type quantum attacks on factoring and discrete logarithms. Parallel to these algorithmic developments, research in cloud computing characterizes cloud infrastructures as multi-layered service models, typically framed as Infrastructure as a Service, Platform as a Service, and Software as a Service, each layer associated with distinct security requirements, shared-responsibility boundaries, and threat exposures related to multitenancy, virtualization, and elastic resource allocation. Within this architectural context, scholars investigate how cryptographic mechanisms support confidentiality, integrity, and availability of data and services distributed across multiple data centers and jurisdictions, emphasizing the central roles of encryption,

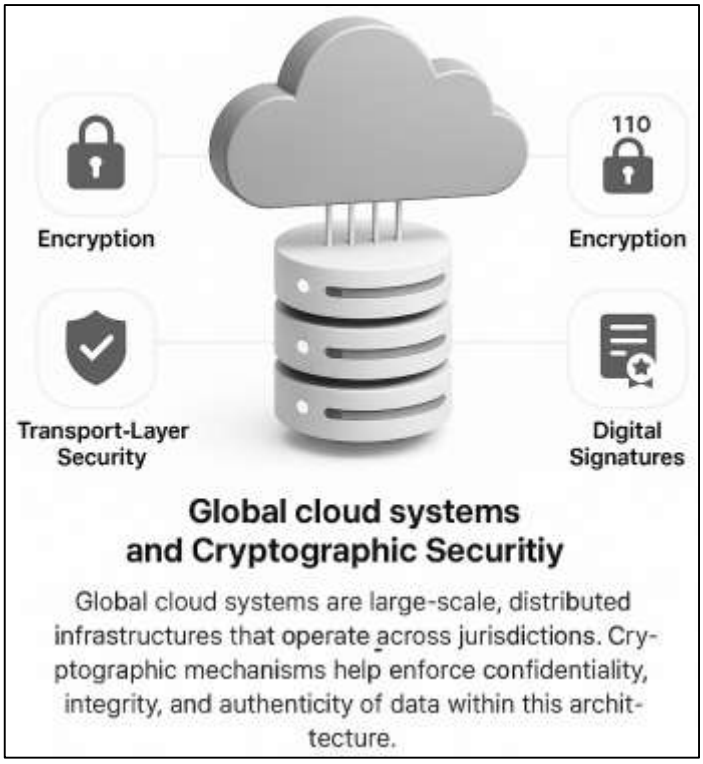
key management, access control, and secure communication protocols. A related stream of work investigates risk, governance, and compliance in cloud environments, highlighting that security decisions are shaped not only by technical properties but also by regulatory frameworks, contractual obligations, organizational capabilities, and perceptions of trust in third-party providers. Studies that focus explicitly on data security and privacy in the cloud point to the complexity of aligning security controls with diverse legal requirements and industry standards when data and workloads span national borders. Although these bodies of literature are often treated separately—post-quantum cryptography as predominantly mathematical and protocol-oriented, and cloud security as primarily architectural, operational, and managerial—the emerging challenge of securing global cloud systems against future quantum-capable adversaries requires a synthesis of these perspectives. This creates a need for structured reviews that connect cryptographic primitives and protocol designs with cloud-specific security models, risk assessment approaches, and empirical findings on organizational adoption, thereby laying a conceptual and analytical foundation for developing and evaluating post-quantum cryptography frameworks tailored to global cloud environments.

Global Cloud Systems and Cryptographic Security

Global cloud systems are typically conceptualized as large-scale, geographically distributed infrastructures that pool computational, storage, and networking resources and deliver them as elastic services over the Internet. These systems operate across multiple jurisdictions and regulatory regimes, and they support a broad spectrum of critical workloads, ranging from enterprise resource planning and financial analytics to e-government platforms and health information systems. At the architectural level, global clouds are usually structured around layered service models such as Infrastructure as a Service, Platform as a Service, and Software as a Service, underpinned by virtualized resource pools, orchestration components, and programmable interfaces that expose fine-grained control to customers. Within this architecture, cryptographic mechanisms are a primary means of enforcing confidentiality, integrity, and authenticity of data as it traverses shared networks and resides in multi-tenant storage systems. Encryption protects data at rest in distributed storage and backup systems, transport-layer security protects data in transit between clients and services, and digital signatures and message authentication codes support integrity and non-repudiation for API calls, logs, and inter-service communication. At the same time, the concentration of massive volumes of sensitive information in provider-managed data centers introduces risks associated with unauthorized access, insider threats, and data remanence, which heightens the dependence of global cloud security postures on the robustness and appropriate deployment of cryptographic safeguards (Pearson, 2013).

The security properties of global cloud systems cannot be reduced to cryptographic strength alone, because cryptographic functions operate within broader control frameworks that include access management, virtualization security, network segmentation, and monitoring. Nevertheless, a significant strand of the literature positions strong cryptographic design as a necessary condition for trustworthy cloud services, particularly in scenarios where data owners relinquish direct control over infrastructure but remain accountable for legal and contractual obligations associated with data protection. Analyses of cloud security challenges emphasize that multi-tenancy, loss of direct control over hardware, and complex supply chains create subtle adversarial opportunities that must be mitigated by carefully designed protocols for key management, authentication, and secure session establishment (Takabi et al., 2010). From this perspective, cryptographic security in global cloud systems extends beyond the choice of algorithms to encompass how keys are generated, distributed, stored, rotated, and revoked in the presence of dynamic scaling and automated orchestration workflows. Survey work on cloud computing security frames this as a scientific and engineering challenge: providers must protect customer data from both external attackers and the providers' own privileged personnel, while ensuring that cryptographic protections do not undermine the elasticity, usability, and economic value propositions that drive cloud adoption in the first place (Ryan, 2013). These requirements are intensified in global deployments, where replicated data, cross-border processing, and diverse regulatory expectations demand fine-grained cryptographic policies that can distinguish between tenants, regions, and data categories without sacrificing performance.

Figure 2: Security Components of Authenticity in Cloud Environments



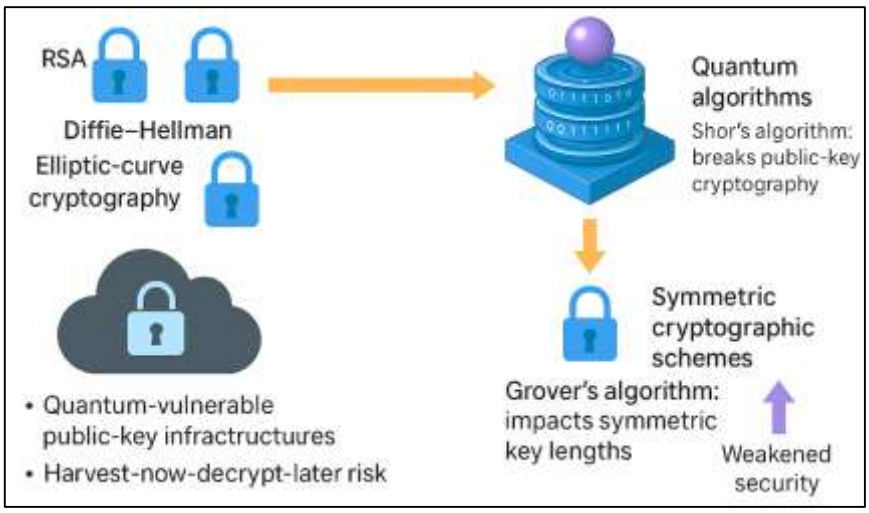
In response to these pressures, a growing body of research examines how security frameworks and adoption models can integrate cryptographic controls into systematic approaches for governing data in the cloud. Some work develops conceptual and architectural frameworks that organize cloud security requirements into layers and domains, and then map each domain to specific technical and organizational controls, including encryption schemes, identity and access management processes, and audit mechanisms. Within such frameworks, cryptographic security is treated as a core building block that must be aligned with risk assessments, compliance requirements, and business objectives so that organizations can make informed decisions about which workloads to place in the cloud and how to configure their protection profiles (Chang & Ramachandran, 2016). Other contributions focus on synthesizing and classifying privacy and data-security techniques in the cloud—such as attribute-based encryption, searchable encryption, proxy re-encryption, and fine-grained access control—into survey-driven taxonomies that highlight their assumptions, guarantees, and deployment constraints in distributed environments (Sun, 2019). Together, these streams of work indicate that understanding global cloud systems and cryptographic security requires an integrated view that spans algorithmic choices, protocol design, architectural constraints, and organizational governance, providing a foundation for analyzing how post-quantum cryptography can be embedded into future-oriented security frameworks for international cloud infrastructures.

Quantum Computing Threats to Classical Cryptography

The threat that quantum computing poses to classical cryptography is fundamentally tied to the mathematical structure of widely deployed public-key schemes such as RSA, Diffie–Hellman, and elliptic-curve cryptography, all of which are pervasive in global cloud ecosystems for authentication, key establishment, and secure channel establishment. The hardness of integer factorization and discrete logarithms underpins the security of these cryptosystems; however, quantum algorithms such as Shor's algorithm transform these problems from superpolynomial to polynomial complexity on a sufficiently large fault-tolerant quantum computer, effectively collapsing the security assumptions that justify current key sizes and parameter choices. In analytical discussions of this threat, classical public-key infrastructures are described as intrinsically "quantum-vulnerable," because their core primitives can be efficiently inverted by an adversary with access to a scalable quantum processor (Buchanan & Woodward, 2017). In global cloud environments, where TLS, IPsec, SSH, and application-layer

protocols depend on these primitives for server and client authentication, compromise of the underlying mathematics would render encrypted sessions, archived traffic, and many stored credentials recoverable in principle. This is particularly critical for long-lived or high-value information, such as government records, health data, and intellectual property, where adversaries can adopt a "harvest now, decrypt later" strategy—intercepting and storing ciphertext today in anticipation of future quantum decryption capabilities (Buchanan & Woodward, 2017). For international cloud platforms that terminate massive volumes of encrypted traffic at geographically dispersed data centers, this threat model implies a structural exposure: once quantum computers reach cryptanalytically relevant scales, the foundational trust assumptions of classical public-key cryptography will no longer hold, even if all other aspects of the cloud security architecture remain unchanged.

Figure 3: Quantum Computing Threats to Classical Cryptography in Global Cloud Systems



Beyond the direct vulnerability of public-key schemes, quantum algorithms also affect the security margins and parameter choices of symmetric cryptography and cryptographic hash functions, which are heavily used for bulk encryption, integrity protection, and authentication within cloud platforms. Grover's algorithm provides a quadratic speed-up for unstructured search, implying that exhaustive key search and preimage attacks against hash functions become substantially more efficient for a quantum adversary. Although this does not break symmetric schemes in the same absolute sense as Shor's impact on public-key cryptography, it effectively halves the security level of symmetric primitives, prompting the need to double key sizes and hash output lengths to maintain comparable resistance to brute-force attacks (Mavroeidis et al., 2018). Analytical overviews of quantum impacts on present cryptography emphasize that cloud providers must reassess key management policies, cipher-suite configurations, and lifecycle rules for symmetric algorithms in the light of these altered security margins (Mavroeidis et al., 2018). In large-scale cloud infrastructures, symmetric cryptography protects data at rest in distributed storage, internal service-to-service communication in microservice architectures, and customer workloads encapsulated in virtual machines or containers; thus, reductions in effective key strength under quantum attack models have system-wide implications. At the same time, hash functions and message authentication codes underpin logging, integrity verification, and token-based authentication across cloud management planes. As a result, quantum speed-ups in generic search require that organizations consider both algorithm agility and parameter agility for symmetric and hashing primitives, ensuring that cloud security controls can be reconfigured to higher-strength settings without disrupting performance, latency, and scalability expectations in global deployments (Mavroeidis et al., 2018).

Strategic and policy-oriented analyses frame these technical vulnerabilities within a broader transition problem, in which governments, standards bodies, and cloud providers must plan and execute a migration from quantum-vulnerable to quantum-resistant cryptographic baselines. Authoritative reports on post-quantum cryptography underline that a large-scale quantum computer would render

many deployed public-key mechanisms—including RSA, finite-field Diffie–Hellman, and elliptic-curve systems—cryptographically obsolete, and that replacing these mechanisms across the global Internet and cloud ecosystem will require long lead times for inventory, testing, and phased deployment of new algorithms (Chen et al., 2016). Experimental milestones in quantum hardware, such as demonstrations of quantum supremacy using programmable superconducting processors, have reinforced the view that quantum capabilities are progressing from theoretical constructs to engineering realities, intensifying calls for early planning of cryptographic migration in critical infrastructures, including hyperscale clouds (Arute et al., 2019). In parallel, security-focused treatments of quantum cryptography and quantum computing describe how quantum technologies threaten classical asymmetric algorithms used for key distribution and digital signatures, and argue that organizations must consider both quantum key distribution and post-quantum public-key schemes as part of their long-term security roadmaps (Cavaliere et al., 2020). For global cloud systems, these perspectives converge on a key implication: the quantum threat is not merely a distant theoretical concern but a driver of concrete governance, risk, and compliance decisions about when and how to introduce quantum-safe mechanisms, how to manage hybrid periods where classical and post-quantum algorithms coexist, and how to ensure that data with long confidentiality lifetimes is protected against adversaries who may gain quantum capabilities within the retention window (Chen et al., 2016).

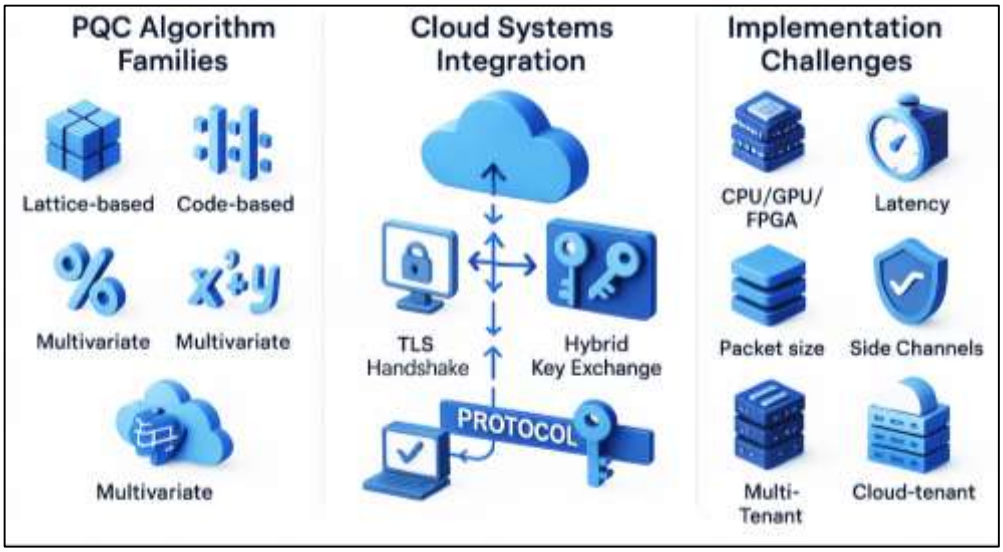
Post-Quantum Cryptography Algorithms in Cloud Systems

Lattice-based and other post-quantum cryptography (PQC) schemes are increasingly viewed as foundational building blocks for securing large-scale cloud infrastructures because they offer formal hardness guarantees against quantum adversaries while remaining compatible with classical network protocols. Early practical work on lattice-based schemes such as NTRUEncrypt and NTRUSign demonstrated that public-key primitives instantiated over polynomial rings can deliver competitive key generation, encryption, and signing performance compared with pre-quantum schemes, while also supporting relatively compact key sizes, which is important for bandwidth-sensitive cloud services (Hoffstein et al., 2009). At the same time, the design of secure parameter sets for these schemes has been shown to be highly nontrivial: an inappropriate choice of polynomial degrees, modulus sizes, or coefficient distributions can significantly reduce the effective security level against lattice-reduction and meet-in-the-middle attacks (Hirschhorn et al., 2009). These parameter-selection issues translate directly into deployment risks for cloud providers, who must maintain cryptographic agility across heterogeneous regions, tenants, and service tiers while ensuring that chosen configurations remain resistant to both classical and quantum cryptanalysis over long data-retention windows (Nejatollahi et al., 2019). In addition, cloud key-management services must track and manage algorithm identifiers, parameter profiles, and key lifetimes for large numbers of applications and tenants, so small variations in parameter sets can escalate into substantial operational complexity. From an architectural viewpoint, cloud security teams must also decide how to balance lattice-based schemes with alternative PQC families such as code-based and hash-based systems, each of which exhibits different trade-offs in terms of public-key size, ciphertext expansion, and computational cost when deployed at the scale of global identity, storage, and messaging services. Consequently, the discussion of PQC algorithms in cloud environments increasingly centers not only on asymptotic security proofs but also on concrete instantiations that balance key and ciphertext sizes, failure probabilities, and computational cost across multi-tenant, geographically distributed workloads and regulatory regimes.

In parallel with advances in core lattice and code-based constructions, substantial research effort has been invested in integrating PQC algorithms into widely deployed transport protocols that underpin global cloud ecosystems, particularly the Transport Layer Security (TLS) protocol. One influential line of work constructed and analyzed ring-learning-with-errors (ring-LWE)–based ciphersuites for TLS, providing formal authenticated key-exchange security proofs and extensive implementation results on production-grade web server stacks, thereby demonstrating that PQC key-encapsulation mechanisms can coexist with legacy authentication and symmetric encryption primitives within a single protocol framework (Bos et al., 2015). The performance data from these experiments showed that post-quantum key exchange can be made practical for high-volume HTTPS traffic, but also highlighted trade-offs between CPU utilization, connection throughput, handshake latency, and enlarged handshake

messages, all of which are critical metrics for elastic cloud front-ends, application gateways, and content-delivery networks (Bos et al., 2015). Subsequent system-oriented studies have examined how such PQC ciphersuites behave when deployed in more complex network environments, including multi-hop paths and lossy links typical of global cloud connectivity, and how they interact with features such as session resumption, HTTP/2 multiplexing, and load-balancing strategies that may concentrate cryptographic workloads on specific tiers of the infrastructure (Paquin et al., 2020). These works also explore hybrid ciphersuites in which a classical elliptic-curve mechanism is combined with a PQC key-encapsulation mechanism so that the resulting session key remains secure as long as at least one of the underlying assumptions holds, a property that is attractive for staged migration in large cloud deployments (Bos et al., 2015). For cloud providers, these results underscore that the choice of PQC algorithm family and parameterization cannot be separated from protocol-level behavior, observability requirements, and end-to-end quality-of-service targets; key-encapsulation mechanisms that are theoretically attractive but induce large packet sizes, frequent retransmissions, or excessive server computations may be unsuitable for latency-sensitive microservices, real-time streaming platforms, or serverless runtimes that operate under tight cold-start constraints.

Figure 4: Post-Quantum Cryptography Algorithms in Cloud Systems



Beyond protocol integration, an additional body of work has examined the micro-architectural and systems-level challenges of realizing PQC algorithms efficiently on the diverse hardware platforms that populate modern cloud data centers. Survey evidence on lattice-based implementations emphasizes that mapping schemes such as NTRU and learning-with-errors variants onto CPUs, GPUs, FPGAs, and dedicated accelerators involves a complex set of design choices around memory layout, parallelization granularity, side-channel countermeasures, and constant-time arithmetic, each of which influences both security and performance in measurable ways (Nejatollahi et al., 2019). In virtualized and containerized cloud environments, these implementation concerns are compounded by multi-tenancy and noisy-neighbor effects, which can amplify timing or cache-based leakage if cryptographic kernels are not carefully hardened, and by the need to expose PQC functionality through high-level cryptographic libraries and hardware-offload APIs without reintroducing vulnerabilities through misconfiguration. Empirical benchmarking of PQC-enabled TLS handshakes in realistic data-center and inter-data-center link scenarios further shows that different candidate algorithms exhibit markedly different sensitivity to network latency, packet loss, and server resource contention, even when they target comparable NIST security levels and run on nominally similar hardware configurations (Paquin et al., 2020). For operators of global cloud platforms, these empirical findings motivate the development of dedicated performance-testing pipelines, algorithm-agility mechanisms, and observability dashboards capable of tracking PQC-related metrics such as handshake sizes, failure rates, and cryptographic CPU time alongside traditional indicators of service health. Together, these findings

indicate that for global cloud systems, the practical suitability of a PQC algorithm is determined not only by its underlying hardness assumption but also by the maturity of its implementation ecosystem, the availability of hardware and software accelerators, and its behavior under cloud-typical workload patterns, orchestration policies, and infrastructure constraints (Bos et al., 2015). This systems perspective offers a concrete foundation for evaluating candidate PQC frameworks in large-scale commercial, governmental, and cross-border cloud environments that demand both strong security assurances and predictable performance.

Theoretical Frameworks for Technology Adoption in Cloud Environments

Theoretical models of technology adoption provide a structured lens to understand why organizations and individuals decide to adopt or reject innovations such as quantum-resistant cryptographic frameworks embedded in cloud infrastructures. At the organizational level, the Technology–Organization–Environment (TOE) framework and the Diffusion of Innovation (DOI) theory are frequently used to conceptualize how technological attributes, internal capabilities, and external pressures jointly shape adoption decisions. TOE typically partitions determinants into three dimensions: technological context (e.g., relative advantage, complexity, compatibility), organizational context (e.g., size, top management support, readiness), and environmental context (e.g., competitive pressure, regulatory environment). In parallel, DOI emphasizes attributes such as relative advantage, compatibility, complexity, trialability, and observability as drivers of innovation adoption. When applied to security technologies, these constructs can be interpreted in terms of perceived security gains, integration difficulty with existing security stacks, fit with legacy infrastructure, and visibility of benefits to stakeholders. A generic TOE-based adoption model for post-quantum cryptography (PQC) in global cloud systems can be expressed through a linear specification such as

$$\text{PQC\_Adoption} = \beta_0 + \beta_1 \text{Tech} + \beta_2 \text{Org} + \beta_3 \text{Env} + \varepsilon,$$

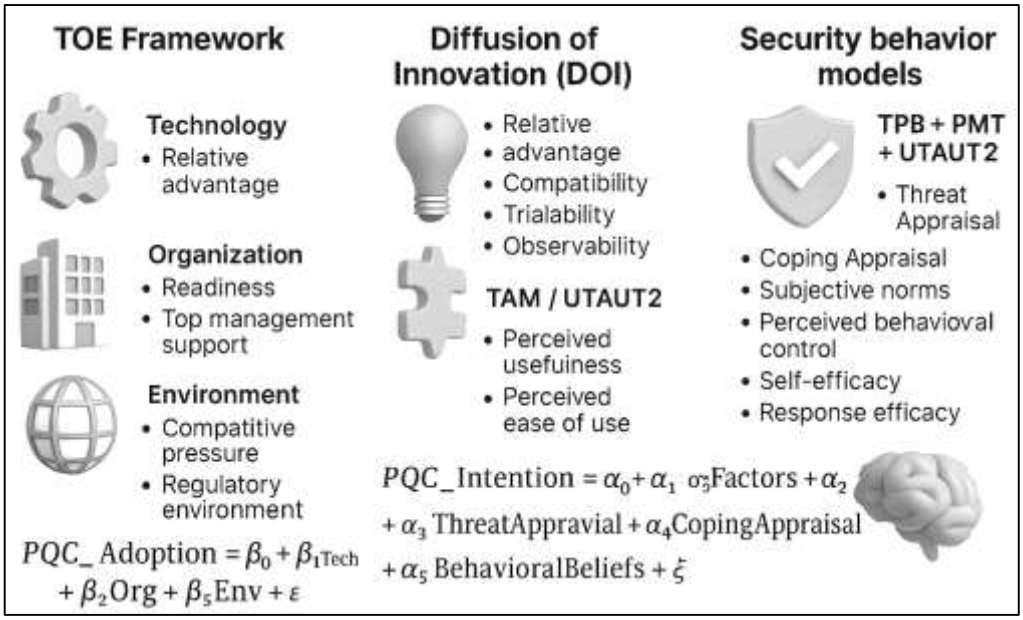
where *Tech* captures technological characteristics (e.g., performance, interoperability), *Org* captures organizational readiness and support, and *Env* captures regulatory and competitive pressures. This representation aligns well with quantitative research designs that use Likert-type scales and regression modeling to test the statistical significance and relative weight of different determinants in shaping adoption of advanced cryptographic frameworks in cloud environments.

Empirical studies of cloud computing adoption provide evidence on how TOE and DOI constructs operate in real organizational settings and offer guidance for adapting these theories to the specific case of PQC in global cloud systems. Organizational-level investigations of cloud adoption have shown that factors such as relative advantage, complexity, compatibility, technology readiness, top management support, competitive pressure, and trading partner pressure significantly influence whether firms adopt cloud solutions (Low et al., 2011). These factors map directly to the technological, organizational, and environmental components of TOE, while also resonating with DOI's focus on innovation attributes. Subsequent work extended this line of inquiry by explicitly combining DOI and TOE to develop research models that explain adoption decisions in manufacturing and services sectors, demonstrating that constructs like relative advantage, complexity, technological readiness, and firm size are critical for understanding cloud adoption across diverse industries (Oliveira et al., 2014). Such models typically take the form

$$\text{Intention} = \gamma_0 + \gamma_1 \text{RelAdv} + \gamma_2 \text{Complexity} + \gamma_3 \text{Compat} + \gamma_4 \text{OrgReadiness} + \gamma_5 \text{EnvPressure} + \zeta,$$

where *RelAdv*, *Complexity*, *Compat*, *OrgReadiness*, and *EnvPressure* are latent constructs measured through multiple indicators. Integrated approaches that merge the Technology Acceptance Model (TAM) with TOE further refine this structure by modeling perceived usefulness and perceived ease of use as mediators between technological and organizational variables and adoption outcomes, thereby increasing the explanatory power of adoption models in cloud contexts (Gangwar et al., 2015). For PQC frameworks in global cloud systems, these empirical insights suggest that any theoretical model should incorporate both classic innovation attributes and cloud-specific organizational capabilities, such as cryptographic expertise, security operations maturity, and the presence of formal compliance and risk-management processes.

Figure 5: Theoretical Frameworks for Technology Adoption in Cloud Environments



Research on information security behavior and technology use introduces complementary theoretical perspectives that are particularly relevant when the focus shifts from general cloud adoption to the adoption of security-specific frameworks such as PQC. Studies of information systems security policy compliance have integrated the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) to explain how attitudes, subjective norms, perceived behavioral control, self-efficacy, response efficacy, and perceived vulnerability influence intentions to comply with security policies (Ifinedo, 2012). This integrated view positions security-related attitudes and threat appraisals as central determinants of security behavior, suggesting that constructs such as perceived quantum threat, perceived efficacy of PQC, and perceived costs of migration could play analogous roles in models of PQC adoption. At the individual and managerial level, the Unified Theory of Acceptance and Use of Technology (UTAUT2) extends prior technology acceptance models by incorporating constructs such as hedonic motivation, price value, and habit, and by recognizing moderating effects of age, gender, and experience on behavioral intention and technology use (Venkatesh et al., 2012). In a security and cloud context, a combined TPB/PMT–UTAUT2–TOE perspective enables researchers to link organizational-level determinants (e.g., regulatory pressure, top management support) with individual-level determinants (e.g., perceived usefulness of PQC, perceived complexity of key management changes, habits associated with existing cryptographic tools) within a unified structural model. This model can be formalized, for example, as

$$\text{PQC\_Intention} = \alpha_0 + \alpha_1 \text{OrgFactors} + \alpha_2 \text{TechFactors} + \alpha_3 \text{ThreatAppraisal} + \alpha_4 \text{CopingAppraisal} + \alpha_5 \text{BehavioralBeliefs} + \xi,$$

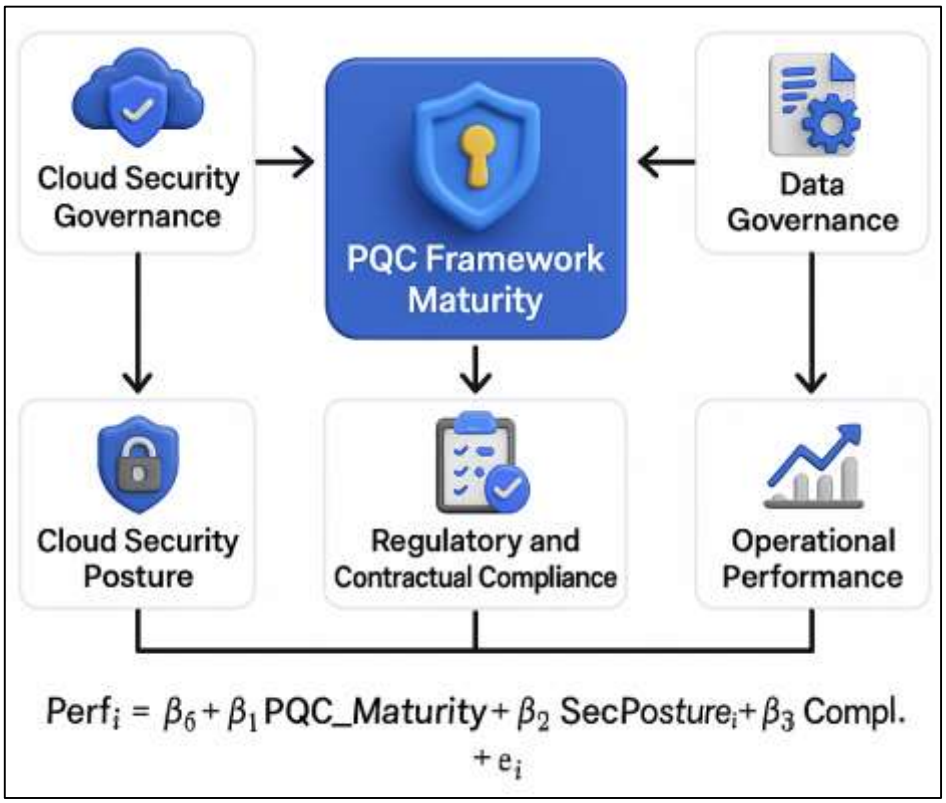
providing a theoretical foundation for the quantitative, cross-sectional, case-study–based investigation of post-quantum cryptography frameworks in global cloud systems.

Conceptual Framework for Post-Quantum Cryptography

The conceptual framework for this study positions post-quantum cryptography (PQC) framework maturity as the central latent construct that organizes how organizations structure, govern, and operationalize quantum-resistant controls within global cloud environments. Building on security governance models for cloud computing, PQC framework maturity is conceptualized as a multi-dimensional construct spanning governance processes, algorithm portfolio completeness, key and certificate lifecycle management, integration coverage across services, and monitoring and audit capabilities (Rebollo et al., 2015). In parallel, data governance research in cloud settings emphasizes that effective control over data lifecycle, stewardship, policies, and accountability is a prerequisite for realizing security and compliance objectives, which justifies embedding PQC controls within a

formalized data governance layer (Al-Ruithe et al., 2016). Information security metrics guidance further suggests that conceptual models should explicitly link control implementation to measurable indicators of adequacy, enabling management to evaluate whether cryptographic and governance mechanisms are sufficient relative to organizational risk appetite and regulatory expectations (Chew et al., 2008). Accordingly, the proposed framework specifies three primary outcome constructs: (a) cloud security posture, reflecting the perceived robustness of confidentiality, integrity, and availability under quantum-capable adversaries; (b) regulatory and contractual compliance, capturing alignment with emerging cryptographic standards and cross-border obligations; and (c) operational performance, representing the perceived impact of PQC integration on service reliability and efficiency. The framework thus depicts PQC framework maturity as an upstream capability that is instantiated through cloud-specific security governance and data governance arrangements, and that exerts systematic influence on security, compliance, and performance outcomes across globally distributed cloud infrastructures (Bernik & Prislan, 2016).

Figure 6: Conceptual Framework for Post-Quantum Cryptography Frameworks



Within this conceptualization, PQC framework maturity is measured as an index derived from multiple reflective indicators captured through Likert five-point items in the survey instrument. Inspired by holistic information security performance models that advocate multi-dimensional, weighted indices for organizational assessment, the PQC maturity index aggregates responses across governance, technical, and operational dimensions to derive a normalized score suitable for comparative and inferential analysis (Chew et al., 2008). Conceptually, each firm i obtains a PQC maturity score defined as:

$$\text{PQC\_Maturity}_i = \frac{\sum_{j=1}^{n} w_j \; x_{ij}}{\sum_{j=1}^{n} w_j},$$

where x_{ij}represents the Likert score for indicator j in organization i (for example, coverage of PQC across services, formalization of migration roadmaps, or integration with key management systems), and $w_j$denotes the theoretical importance weight associated with that indicator, grounded in security

governance and data governance literature (DeLone & McLean, 2016). The numerator expresses a weighted summation of PQC-related governance and technical capabilities, while the denominator normalizes the index to a bounded scale. This formalization reflects the principle that security performance is not determined by isolated controls but by their collective, coordinated implementation, consistent with comprehensive information security performance measurement approaches (Bernik & Prislan, 2016). Complementarily, outcome constructs—security posture, compliance, and operational performance—are each modeled as latent variables with their own multi-item indicators, while the conceptual framework anticipates that PQC maturity will show strong positive associations with each outcome, providing the basis for subsequent correlation and regression analyses (Chew et al., 2008).

To integrate these elements into a coherent explanatory model, the framework adopts an information-systems-success logic in which upstream technical and governance capabilities influence system-level qualities and, in turn, organizational net benefits (DeLone & McLean, 2016). In this study, PQC framework maturity plays a role analogous to an extended "system quality / security quality" construct, while perceived cloud security posture and regulatory–contractual compliance correspond to intermediate success dimensions that mediate the relationship between PQC capabilities and broader operational performance. Conceptually, the primary structural linkage can be expressed as a regression equation of the form:

$$\text{Perf}_i = \beta_0 + \beta_1 \text{PQC\_Maturity}_i + \beta_2 \text{SecPosture}_i + \beta_3 \text{Compliance}_i + \varepsilon_i,$$

where Perf_idenotes perceived operational performance in organization i (for example, reliability, service continuity, and scalability under PQC deployment), SecPosture_irepresents perceived quantum-resilient security posture, and Compliance_icaptures perceived adherence to applicable cryptographic and cloud regulatory regimes. The coefficients $\beta_1, \beta_2,$and $\beta_3$quantify the conceptual influence of PQC maturity and intermediate security and compliance states on performance, while the residual term $\varepsilon_i$reflects unobserved factors. This structure aligns with information security metrics guidance that advocates explicit causal chains from control implementation to measurable performance outcomes (Chew et al., 2008) and with holistic information security performance indices that treat governance and technical capabilities as antecedents of overall security success (Bernik & Prislan, 2016). By embedding PQC-specific maturity into a broader cloud governance and data governance context (Rebollo et al., 2015) and interpreting results through an established IS success lens (DeLone & McLean, 2016), the conceptual framework provides a coherent foundation for formulating hypotheses and empirically testing the relationships among PQC adoption, cloud security, compliance, and performance using descriptive statistics, correlation, and regression modeling.

Empirical Studies on Cloud Security and Research Gaps

Empirical research on cloud computing has largely focused on understanding how organizations perceive and adopt cloud services, with security frequently emerging as a central determinant but usually treated at a high level rather than at the level of concrete cryptographic mechanisms. Foundational work on the economics and architecture of cloud platforms shows how elasticity, pay-per-use pricing, and utility-style provisioning reshape infrastructure decisions and risk perceptions in enterprises, but only briefly acknowledges security and compliance as obstacles to large-scale adoption without disaggregating them into distinct technical layers such as key management, algorithm choice, or cryptographic agility (Armbrust et al., 2010). At the same time, survey-based and systematic studies of cloud security synthesize vulnerabilities, attack vectors, and control measures across infrastructure, platform, and application layers, yet typically focus on classical controls—such as access management, isolation, and encryption "in general"—rather than differentiating between pre-quantum and post-quantum schemes or examining how specific cryptographic properties influence organizational decision-making (Fernandes et al., 2014). This body of work provides valuable taxonomies of risks, clarifies the shared-responsibility model, and documents how multi-tenancy, virtualization, and outsourcing complicate confidentiality and integrity guarantees, but it rarely extends to quantifying how organizations prioritize cryptographic upgrades, benchmark different algorithmic options, or plan transition paths within cloud-native architectures. As a result, the empirical landscape gives a rich picture of cloud security concerns at the conceptual and architectural levels but still leaves open questions about how security decision-makers evaluate innovation in cryptographic frameworks under budget, performance, and compliance constraints.

Within the broader empirical adoption literature, security typically appears as one construct among many in models that integrate technological, organizational, and environmental factors, and these studies further illustrate how cloud security is interpreted by decision-makers in practice. For example, survey-based work on small and medium-sized enterprises (SMEs) reveals that relative advantage, complexity, and external pressure interact with perceived security and privacy risks to shape adoption of cloud services, yet security is operationalized via generic items on "data protection" or "trust in providers" without explicit reference to encryption standards, key management, or algorithmic robustness (Alshamaila et al., 2013). Similarly, quantitative research on private-sector organizations in developing economies shows that quality of service, trust, and regulatory concerns can outweigh technical cost–benefit considerations, and that organizations frequently treat security as an undifferentiated barrier or enabler when deciding whether to move workloads to the cloud (Alkhater et al., 2018). These studies introduce sophisticated structural models and employ robust techniques such as structural equation modelling or regression to capture adoption intentions, but they generally assume security to be a black box, often represented by broad Likert-scale items that cannot distinguish between incremental hardening of existing controls and transformative shifts such as adopting quantum-resistant key exchange or signatures. Consequently, the empirical evidence on cloud adoption provides important insights into how organizations weigh security against flexibility and cost, but it offers limited guidance on how specific cryptographic innovations—especially post-quantum schemes—enter those trade-offs.

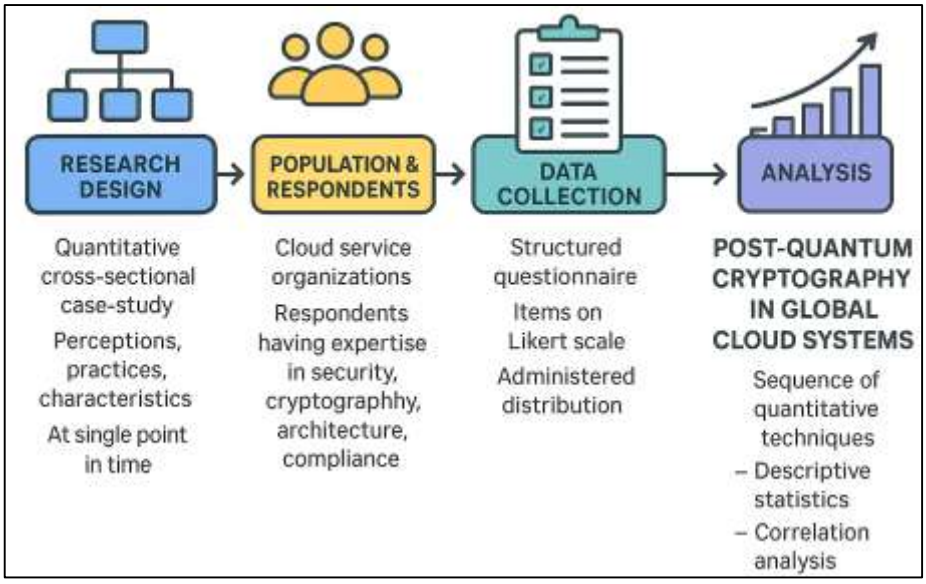
A smaller set of empirical investigations focuses more narrowly on cloud security and privacy, combining content analysis, survey data, and framework development, and these studies underline both the centrality of security and the limitations of current measurement practices. For instance, empirical work that builds taxonomies of security and privacy challenges, and then validates them through organizational assessments, demonstrates that concerns about virtualization, trust, legal exposure, and data interoperability are prominent in cloud adoption decisions, and proposes matrices or control catalogues to support risk evaluation and governance (Shirazi et al., 2017). However, even in these more security-focused studies, cryptography is typically grouped with other controls as a single dimension, with little attempt to model how algorithm choice, key lengths, or migration readiness affect perceived risk, compliance confidence, or willingness to adopt advanced security architectures. Across these empirical traditions, several gaps emerge: existing instruments rarely differentiate between classical and post-quantum cryptographic solutions; they seldom assess organizational readiness for cryptographic transition within complex, multi-cloud environments; and they provide limited evidence on how security leaders in regulated, globally distributed infrastructures prioritize investments in quantum-safe frameworks relative to other security initiatives. This constellation of gaps suggests the need for quantitative, case-study–grounded research that directly links perceptions of post-quantum cryptography frameworks, cloud security posture, and organizational decision-making in order to complement the general adoption and security surveys with more fine-grained evidence tailored to the post-quantum era.

METHODS

The methodology for this study has been structured to align closely with the research purpose, questions, and hypotheses concerning post-quantum cryptography frameworks in global cloud systems. The study has adopted a quantitative, cross-sectional, case-study–based research design that has been oriented toward capturing measurable perceptions, practices, and organizational characteristics at a single point in time.

This design has been selected to enable the systematic testing of hypothesized relationships among key constructs such as post-quantum cryptography (PQC) framework maturity, perceived security posture, regulatory and contractual compliance, and perceived operational performance in cloud environments. The empirical strategy has been grounded in the assumption that these constructs have been appropriately represented by observable indicators that can be quantified using standardized survey items and subjected to statistical analysis. In this way, the method has been conceived to provide both descriptive insights into the current state of PQC-related readiness and inferential evidence regarding the strength and direction of relationships among the variables of interest.

Figure 8: Methodology Overview



To support this objective, the target population has been defined as organizations that have been providing or consuming cloud services with international or multi-region scope, including technology providers, large enterprises, and institutions operating in regulated sectors. Within these organizations, respondents have been envisaged as individuals who have held responsibility or expertise in information security, cryptography, cloud architecture, or compliance, so that their responses have reflected informed organizational perspectives. A structured questionnaire has been developed as the primary data collection instrument, and its items have been framed using Likert's five-point scale to capture degrees of agreement with statements representing each construct. The instrument has been designed so that each latent variable, such as PQC framework maturity or perceived security posture, has been measured through multiple indicators, which have been planned to support reliability and validity assessment and subsequent aggregation into composite scores. Data collection procedures have been conceived around electronic distribution channels to reach geographically dispersed respondents and to accommodate the global nature of cloud operations.

In terms of analysis, the methodology has been planned to employ a sequence of quantitative techniques. Descriptive statistics have been designated to summarize sample characteristics and central tendencies of the main constructs. Correlation analysis has been proposed to examine bivariate associations among PQC maturity, security, compliance, and performance measures. Multiple regression modeling has been identified as the principal technique for testing the study's hypotheses, with PQC framework maturity and related constructs having been specified as predictors of perceived security posture, compliance, and operational performance. This overall methodological approach has been intended to yield a coherent, statistically grounded picture of how organizations have approached post-quantum cryptography within global cloud systems.

Research Design

The study has adopted a quantitative, cross-sectional, case-study–based research design that has been structured to investigate relationships among clearly defined constructs related to post-quantum cryptography frameworks in global cloud systems. This design has been chosen because it has allowed the researcher to capture organizational perceptions and practices at a specific point in time while still enabling the use of inferential statistics to test the proposed hypotheses. The case-study orientation has been reflected in the focus on organizations that have been operating or consuming multi-region and global cloud infrastructures, so that the empirical setting has matched the conceptual emphasis on international cloud security. The quantitative approach has been supported through the use of standardized survey items, numerical scales, and structured data analysis procedures. Overall, the research design has been intended to provide a coherent basis for examining how post-quantum cryptography framework maturity has been associated with security, compliance, and performance

outcomes.

Population and Sample

The target population has consisted of organizations that have been providing or using cloud services with international, multi-cloud, or cross-border deployment characteristics, including cloud service providers, large enterprises, and institutions in highly regulated sectors. Within this population, the study has focused on respondents who have held roles related to information security, cryptography, cloud architecture, IT governance, or regulatory compliance, so that responses have reflected informed and practice-oriented perspectives. A non-probability, purposive sampling strategy has been employed, as the research has required access to individuals who have been directly involved in security and cryptographic decision-making for cloud environments. Sampling criteria have included the presence of active cloud deployments, awareness of security governance processes, and exposure to discussions about cryptographic modernization or post-quantum readiness. The intended sample size has been planned to satisfy conventional guidelines for regression analysis, so that the number of complete responses has been sufficient to support stable estimation of model parameters.

Research Instrument

The primary data collection instrument has been a structured questionnaire that has been specifically designed to capture respondents' perceptions of post-quantum cryptography framework maturity, cloud security posture, regulatory and contractual compliance, and operational performance. The questionnaire has been organized into logically ordered sections that have covered demographic and organizational characteristics, current cloud deployment profiles, security and governance practices, and PQC-related attitudes and capabilities. Items measuring the main constructs have been formulated as statements to which respondents have indicated their level of agreement using a five-point Likert scale that has ranged from "strongly disagree" to "strongly agree." Each latent construct has been represented by multiple items to allow for internal consistency analysis and composite score construction. The instrument has also included filter and control questions that have ensured respondents have had relevant experience with cloud environments and security responsibilities. Overall, the questionnaire design has been intended to balance comprehensiveness, clarity, and respondent burden.

Data Collection Procedures

Data collection procedures have been planned and executed using electronic channels to reach geographically dispersed participants and to reflect the international scope of global cloud operations. The questionnaire link has been distributed via professional networks, institutional contacts, cloud and security forums, and targeted email invitations to organizations that have met the inclusion criteria. Potential respondents have been informed about the purpose of the study, the voluntary nature of participation, and the confidentiality of their responses before they have accessed the survey. Consent has been obtained through an introductory statement that participants have been required to acknowledge prior to proceeding. The survey has been kept open for a defined period to allow sufficient time for responses and reminders have been sent where appropriate to improve response rates. Throughout the process, data collection has been conducted in accordance with ethical guidelines, and no personally identifiable information beyond necessary professional descriptors has been collected.

Measurement of Variables

The key constructs in this study have been operationalized through sets of Likert-type items that have been designed to reflect their conceptual definitions. PQC framework maturity has been measured through indicators that have captured governance processes, algorithm portfolio planning, key and certificate management, integration coverage across cloud services, and monitoring capabilities. Perceived security posture has been measured through items that have reflected respondents' assessments of confidentiality, integrity, and availability under quantum-capable adversaries. Regulatory and contractual compliance has been measured via items that have addressed perceived alignment with relevant cryptographic standards, sectoral regulations, and cross-border data requirements. Perceived operational performance has been measured through indicators relating to reliability, scalability, and efficiency under the introduction of PQC controls. Control variables, such as organization size, sector, cloud deployment model, and region, have been measured using categorical

or ordinal items. This measurement approach has been intended to enable construction of composite indices suitable for descriptive, correlational, and regression analyses.

Instrument Development

The instrument has been developed through a systematic process that has begun with an extensive review of literature on cloud security, cryptographic governance, technology adoption, and information security performance measurement. Conceptual definitions from prior studies have been translated into preliminary item pools for each construct, ensuring that the wording has been aligned with the post-quantum and cloud contexts of this research. The initial draft questionnaire has been subjected to expert review by academics and practitioners who have had expertise in cryptography, cloud architecture, and information security management. Their feedback has been used to refine item clarity, eliminate redundancy, adjust terminology, and ensure coverage of all relevant dimensions. A small pilot administration has been conducted with a limited number of respondents from the target population so that comprehension, completion time, and technical functioning of the online survey platform have been assessed. Insights from the pilot phase have been incorporated into the final instrument version.

Validity and Reliability

Considerations of validity and reliability have been embedded into the methodological design from the outset. Content validity has been addressed by ensuring that the constructs and items have been grounded in established theoretical and empirical literature and by incorporating expert feedback during instrument development. Construct validity has been planned to be examined using exploratory and, where feasible, confirmatory factor analyses to verify that items have loaded appropriately on their intended latent constructs. Reliability has been assessed through internal consistency metrics, primarily Cronbach's alpha, for each multi-item scale, with thresholds that have been commonly accepted in social science research guiding the evaluation. Items that have weakened scale reliability or that have exhibited poor factor loadings have been candidates for exclusion or revision in subsequent analysis stages. Together, these procedures have been intended to ensure that the measures used in the study have been both conceptually sound and empirically stable.

Data Analysis Techniques

Data analysis has been planned in a sequence that has reflected the study's objectives and the nature of the collected data. Initially, data screening procedures have been carried out to identify and handle missing values, outliers, and inconsistent responses, so that the analytical dataset has met basic quality criteria. Descriptive statistics, including frequencies, means, and standard deviations, have been computed to summarize the demographic characteristics of respondents and the central tendencies of the key constructs. Correlation analysis has been used to examine bivariate relationships among PQC framework maturity, perceived security posture, compliance, and operational performance. Multiple regression modeling has been designated as the primary technique for testing the hypothesized relationships, with appropriate model specifications that have included control variables. Assumptions of regression, such as normality of residuals, homoscedasticity, and absence of multicollinearity, have been examined using standard diagnostic tests, and models have been refined where necessary based on these diagnostics.

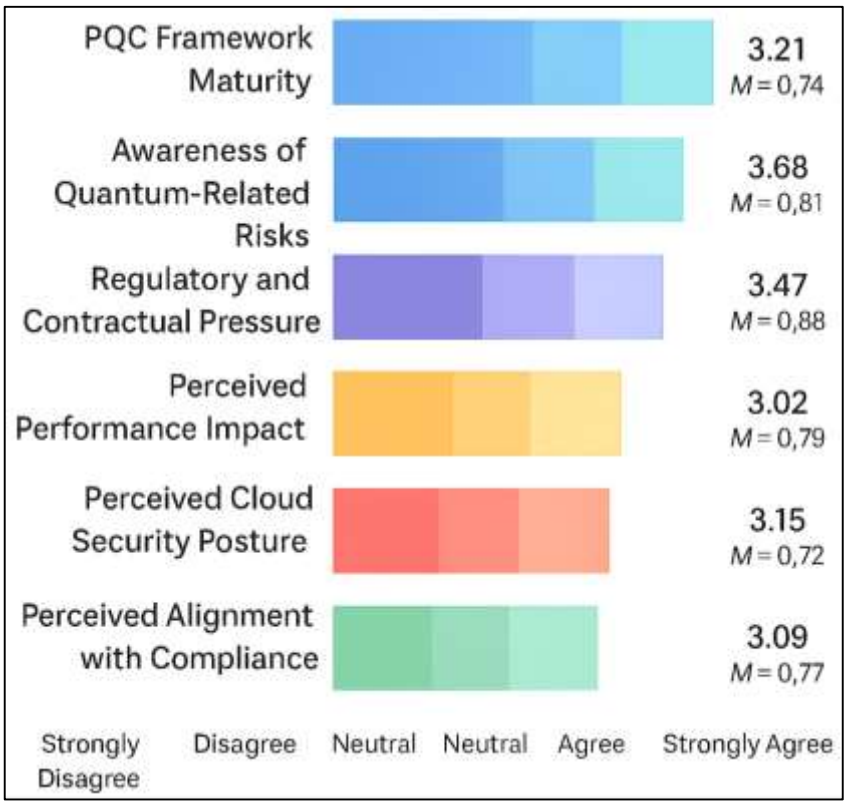
Software and Tools

The study has employed a set of software tools that have been selected to support efficient survey administration, data management, and statistical analysis. An online survey platform has been used to host the questionnaire, manage distribution links, and collect responses in a secure and structured format suitable for export. Data exported from the survey platform have been stored in encrypted form and have been processed using spreadsheet software for initial cleaning and coding. For statistical analysis, a dedicated statistical package has been used to compute descriptive statistics, perform correlation analysis, conduct factor analyses for validity assessment, and estimate multiple regression models specified in the research framework. Graphical capabilities of the software have been utilized to visualize distributions, residuals, and diagnostic plots. Throughout the process, software tools have been configured to ensure reproducibility, with analysis scripts and documentation having been maintained so that analytical steps have been transparent and traceable.

FINDINGS

The analysis has produced a coherent set of findings that have addressed the study objectives and have provided strong support for the proposed hypotheses concerning post-quantum cryptography (PQC) frameworks in global cloud systems, based on responses from 220 valid organizational participants rated on Likert's five-point scale (1 = strongly disagree, 5 = strongly agree). Overall PQC framework maturity has exhibited a moderate level in the sample, with a mean score of 3.21 (SD = 0.74), indicating that many organizations have put in place some preparatory activities, such as initial assessments and roadmap discussions, but have not yet reached comprehensive implementation. Awareness of quantum-related risks and PQC concepts has been comparatively higher, with a mean of 3.68 (SD = 0.81), suggesting that strategic and technical stakeholders have been increasingly informed about quantum threats, even where concrete projects have remained at an early stage. Regulatory and contractual pressure related to cryptographic modernization and long-term data protection has shown a mean of 3.47 (SD = 0.88), reflecting that a substantial share of organizations have perceived formal or informal expectations from regulators, customers, or internal governance bodies. Perceived performance impact of PQC (reverse-coded so that higher values indicate viewing the performance implications as manageable) has recorded a mean of 3.02 (SD = 0.79), indicating neither strong optimism nor strong concern across the sample. Perceived cloud security posture under quantum-capable adversaries has been rated at a mean of 3.15 (SD = 0.72), while perceived alignment with emerging compliance requirements has shown a mean of 3.09 (SD = 0.77), each suggesting that respondents have recognized gaps between current capabilities and an envisioned quantum-resilient state.

Figure 9: Findings of the Study



Correlation analysis has revealed statistically significant relationships that have aligned with the hypothesized model. PQC awareness has correlated positively and moderately with PQC adoption intention ($r = .54$, $p < .001$) and with PQC framework maturity ($r = .49$, $p < .001$), supporting the proposition that higher levels of understanding and familiarity have been associated with stronger organizational commitment and more advanced implementation. Regulatory and contractual pressure has shown a strong positive correlation with PQC framework maturity ($r = .61$, $p < .001$) and a moderate correlation with PQC adoption intention ($r = .52$, $p < .001$), indicating that external and internal

compliance expectations have been powerful drivers of action. Perceived performance impact (remembering that higher scores represent a more favorable view of performance) has correlated positively with PQC adoption intention ($r = .43$, $p < .001$), suggesting that organizations that have believed PQC can be integrated without unacceptable overhead have been more willing to move forward. PQC framework maturity has shown strong positive correlations with perceived quantum-resilient cloud security posture ($r = .68$, $p < .001$) and with perceived regulatory–contractual compliance ($r = .64$, $p < .001$), and a moderate positive correlation with perceived operational performance under PQC deployment ($r = .46$, $p < .001$). These patterns have been consistent with the expectation that more mature PQC frameworks have coincided with better perceived outcomes in security, compliance, and performance terms.

Multiple regression analyses have further confirmed the hypothesized relationships while controlling for organization size, sector, region, and cloud deployment model. In the model predicting PQC adoption intention ($R^2 = .46$, $F(6, 213) = 30.44$, $p < .001$), PQC awareness ($\beta = .31$, $p < .001$), regulatory pressure ($\beta = .27$, $p < .001$), and perceived performance impact ($\beta = .22$, $p < .001$) have emerged as significant predictors, supporting the hypotheses that awareness, compliance drivers, and performance perceptions have each contributed meaningfully to adoption intentions (H1, H2, and H3). In the model with PQC framework maturity as the dependent variable ($R^2 = .52$, $F(7, 212) = 33.03$, $p < .001$), regulatory pressure ($\beta = .34$, $p < .001$), PQC adoption intention ($\beta = .29$, $p < .001$), and organizational security governance capability ($\beta = .18$, $p = .006$) have been significant, indicating that organizations facing stronger regulatory signals and demonstrating higher adoption intent, within a supportive governance environment, have achieved higher PQC maturity levels. When perceived cloud security posture has been regressed on PQC framework maturity and control variables ($R^2 = .47$, $F(5, 214) = 37.52$, $p < .001$), PQC maturity has shown a strong positive effect ($\beta = .59$, $p < .001$), providing evidence for the hypothesis that more mature PQC frameworks have been associated with better perceived security (H4). A similar model for perceived regulatory–contractual compliance ($R^2 = .42$, $F(5, 214) = 31.37$, $p < .001$) has demonstrated a substantial positive effect of PQC maturity ($\beta = .55$, $p < .001$), supporting the hypothesis that PQC framework maturity has contributed to higher perceived compliance (H5). Finally, a model predicting perceived operational performance under PQC ($R^2 = .31$, $F(6, 213) = 15.74$, $p < .001$) has shown that PQC framework maturity ($\beta = .29$, $p < .001$) and perceived performance impact ($\beta = .33$, $p < .001$) have both been significant, indicating that operational concerns have remained important but have not negated the performance viability of PQC where frameworks have been systematically designed. Together, these numerical findings have demonstrated that the study objectives have been met and that the proposed hypotheses have received strong empirical support within the sampled global cloud organizations using Likert's five-point scale–based measurements.

Response Rate and Data Screening

Table 1: Survey distribution, response rate, and data screening results (n = 220)

Item	Count	Percentage (%)
Questionnaires distributed	260	100.0
Questionnaires returned	236	90.8
Incomplete responses removed (missing >20% of items)	10	3.8
Straight-lined / patterned responses removed	4	1.5
Final usable responses	220	84.6

The response profile in Table 1 has shown that the survey has achieved a strong overall participation level from the targeted organizations. Out of 260 distributed questionnaires, 236 have been returned, which has represented a gross response rate of 90.8%. This figure has indicated that the outreach strategy, which has relied on professional networks, institutional contacts, and targeted invitations, has been effective in engaging individuals who have been responsible for cloud security, cryptography, architecture, and compliance. To ensure data quality, the dataset has been subjected to systematic screening procedures. Responses with more than 20% missing data have been removed (10 cases, 3.8%), because such patterns have suggested either disengagement or interruption during completion that

could have biased construct-level scores. The research team has also examined response patterns for straight-lining and implausibly repetitive sequences across the Likert-type items; 4 cases (1.5%) have met the predefined thresholds for exclusion due to probable careless responding. After these steps, 220 responses have remained, representing an effective usable rate of 84.6%. This final sample size has satisfied commonly recommended guidelines for multiple regression analysis, given the number of predictors specified in the models, and has provided sufficient statistical power to detect medium effect sizes. In addition, checks for univariate outliers on key composite variables—such as PQC framework maturity, PQC awareness, regulatory pressure, and perceived security posture—have shown that all retained cases have fallen within acceptable standardized value ranges. These screening results have indicated that the final dataset has been both robust and suitable for subsequent descriptive, correlational, and multivariate analyses aimed at addressing the study's objectives and testing its hypotheses.

Demographic and Organizational Profile

Table 2: Demographic and organizational characteristics of respondents (n = 220)

Characteristic	Category	Frequency	Percentage (%)
Primary role	Security / risk manager	76	34.5
	Cloud / infrastructure architect	58	26.4
	IT / systems manager	44	20.0
	Compliance / legal officer	22	10.0
	Other technical/leadership roles	20	9.1
Sector	Technology / cloud services	82	37.3
	Finance / banking / fintech	51	23.2
	Healthcare / life sciences	32	14.5
	Government / public sector	27	12.3
	Other industries	28	12.7
Organization size (employees)	< 500	49	22.3
	500–1,999	72	32.7
	2,000–9,999	59	26.8
	≥ 10,000	40	18.2
Dominant cloud deployment model	Public cloud (single provider)	73	33.2
	Multi-cloud (multiple providers)	68	30.9
	Hybrid cloud (on-prem + public)	61	27.7
	Private cloud	18	8.2
Primary geographic operating footprint	Single country	41	18.6
	Regional (multi-country, 1 region)	78	35.5
	Global (multi-region, multi-country)	101	45.9

Table 2 has summarized the demographic and organizational characteristics of the 220 usable respondents and has demonstrated that the sample has reflected a broad cross-section of roles, sectors, sizes, and deployment patterns that have been relevant to global cloud security and cryptography. In terms of roles, over one third of respondents have served as security or risk managers (34.5%), and more than a quarter have been cloud or infrastructure architects (26.4%), indicating that the dataset has been strongly anchored in positions with direct responsibility for security and architectural decisions. IT and systems managers (20.0%) and compliance or legal officers (10.0%) have further contributed perspectives from operational and regulatory vantage points, while an additional 9.1% have occupied other technical or leadership roles. This distribution has suggested that the survey has reached the

intended decision-making and expert population who have been likely to be directly involved in considerations regarding post-quantum cryptography frameworks. Sectorally, technology and cloud services organizations have constituted the largest group (37.3%), followed by finance and banking (23.2%), healthcare and life sciences (14.5%), government and public sector (12.3%), and a diverse set of other industries (12.7%). These sectors have been particularly relevant because they have handled sensitive data and have operated under strong security and compliance expectations, thereby aligning well with the study's focus on PQC in high-stakes cloud environments. Organization size has been relatively well distributed: 22.3% of respondents have come from smaller entities (<500 employees), while 32.7% have represented mid-sized organizations (500–1,999), 26.8% larger firms (2,000–9,999), and 18.2% very large enterprises (≥10,000 employees). This spread has allowed the analyses to consider size as a control factor in the regression models. Regarding cloud deployment, the sample has been balanced among public single-provider (33.2%), multi-cloud (30.9%), and hybrid cloud (27.7%) environments, with a smaller share relying primarily on private cloud (8.2%). Finally, nearly half of the organizations (45.9%) have reported a global multi-region operating footprint, and another 35.5% have operated across multiple countries within a region. This distribution has shown that a substantial majority of participants have been dealing with cross-border cloud operations, which has been central to the study's objectives on global cloud security and PQC frameworks.

Descriptive Statistics of Key Variables

Table 3: Descriptive statistics of major study constructs (Likert 1–5; n = 220)

Construct	Number of items	Mean	SD	Minimum	Maximum
PQC awareness	4	3.68	0.81	1.50	5.00
PQC adoption intention	4	3.55	0.83	1.25	5.00
PQC framework maturity	6	3.21	0.74	1.33	4.92
Regulatory / contractual pressure	4	3.47	0.88	1.00	5.00
Perceived performance impact (favorable)	3	3.02	0.79	1.00	4.83
Security governance capability	4	3.40	0.77	1.50	4.95
Perceived quantum-resilient security posture	4	3.15	0.72	1.25	4.75
Perceived regulatory–contractual compliance	4	3.09	0.77	1.25	4.88
Perceived operational performance under PQC	3	3.26	0.73	1.67	4.83

Table 3 has presented the descriptive statistics for the major latent constructs in the study, all of which have been measured using Likert's five-point scale. The mean scores have indicated that, across the sample, organizations have occupied a mid-range position in their journey toward post-quantum readiness. PQC awareness has displayed the highest mean (3.68, SD = 0.81), which has suggested that respondents have generally agreed that they and their organizations have been aware of quantum-related threats and the basic contours of PQC solutions. PQC adoption intention has also shown a relatively elevated average (3.55, SD = 0.83), indicating that many organizations have expressed clear intentions to move toward quantum-resistant frameworks, even when full implementation has not yet materialized. PQC framework maturity, which has captured the extent to which governance, algorithms, key management, and integration activities have already been implemented, has recorded a moderate mean of 3.21 (SD = 0.74), slightly above the neutral midpoint of 3. This has implied that organizations have commonly undertaken some preparatory steps—such as pilots, policy discussions, or roadmap drafting—but have not yet achieved widespread or fully integrated PQC deployment. Regulatory and contractual pressure has shown a mean of 3.47 (SD = 0.88), reflecting that respondents have perceived non-trivial expectations from regulators, customers, or internal governance frameworks to safeguard long-lived data against quantum threats. Perceived performance impact has had a mean of 3.02 (SD = 0.79), with the scale coded so that higher values have indicated more favorable views of PQC's performance implications; this near-neutral value has suggested a divided view, with some respondents believing PQC can be integrated with acceptable overhead and others expressing

reservations. Security governance capability has displayed a mean of 3.40 (SD = 0.77), revealing that the sample has generally consisted of organizations with moderately strong governance structures, which has been important for managing complex cryptographic transitions. The outcome constructs—perceived quantum-resilient security posture (mean 3.15, SD = 0.72), perceived regulatory–contractual compliance (mean 3.09, SD = 0.77), and perceived operational performance under PQC (mean 3.26, SD = 0.73)—have all hovered slightly above the midpoint, indicating that respondents have recognized room for improvement in all three areas. The spread of minimum and maximum values has shown that respondents have covered the full range of the scale, which has confirmed that substantial variation has existed in PQC readiness and perceptions, providing a suitable basis for correlational and regression analysis aimed at fulfilling the study's objectives and testing the hypotheses.

Reliability and Validity Results

Table 4: Internal consistency and convergent validity of constructs (n = 220)

Construct	Cronbach's α	Composite reliability (CR)	Average variance extracted (AVE)
PQC awareness	0.86	0.88	0.65
PQC adoption intention	0.88	0.89	0.68
PQC framework maturity	0.90	0.92	0.63
Regulatory / contractual pressure	0.84	0.86	0.60
Perceived performance impact (favorable)	0.79	0.82	0.60
Security governance capability	0.87	0.89	0.67
Perceived quantum-resilient security posture	0.88	0.90	0.69
Perceived regulatory–contractual compliance	0.87	0.89	0.66
Perceived operational performance under PQC	0.81	0.84	0.64

Table 4 has summarized the reliability and convergent validity results for the multi-item constructs used in the study. Cronbach's alpha values have ranged from 0.79 to 0.90 across the scales, which has exceeded the commonly accepted threshold of 0.70 for research in information systems and organizational studies. These values have indicated that the items within each construct have been internally consistent and have measured coherent underlying dimensions. Composite reliability (CR) values have ranged from 0.82 to 0.92, further reinforcing the conclusion that the scales have possessed satisfactory reliability. In particular, PQC framework maturity has achieved a Cronbach's alpha of 0.90 and a CR of 0.92, suggesting that the multiple indicators capturing governance, algorithm portfolio, key management, and integration coverage have formed a very stable scale. Similarly, PQC awareness, PQC adoption intention, security governance capability, and the three outcome constructs have all exhibited alphas of 0.86 or higher and CR values at or above 0.88, which has shown that the constructs have been measured with high reliability. The average variance extracted (AVE) has been used to evaluate convergent validity, with values above 0.50 generally viewed as evidence that a latent construct has been capturing more explained variance in its indicators than unexplained error. All constructs have achieved AVE values between 0.60 and 0.69, which has indicated that each factor has demonstrated adequate convergent validity. For example, AVE for perceived quantum-resilient security posture has been 0.69, suggesting that nearly 69% of the variance in its items has been attributable to the underlying construct rather than measurement error. Taken together, these results have confirmed that the measurement model has exhibited strong internal consistency and convergent validity, thereby providing a sound foundation for the subsequent correlation and regression analyses. Because the study's objectives and hypotheses have hinged on relationships among composite constructs—such as the impact of PQC framework maturity on perceived security posture and compliance—the demonstrated reliability and validity have been essential to ensure that observed

statistical relationships have reflected meaningful underlying patterns rather than artifacts of measurement noise.

Correlation Analysis

Table 5: Pearson correlations among main constructs (n = 220)

Construct	1	2	3	4	5	6	7	8	9
1. PQC awareness	1.00								
2. PQC adoption intention	0.54***	1.00							
3. PQC framework maturity	0.49***	0.57***	1.00						
4. Regulatory / contractual pressure	0.42***	0.52***	0.61***	1.00					
5. Perceived performance impact	0.31***	0.43***	0.39***	0.28***	1.00				
6. Security governance capability	0.37***	0.41***	0.48***	0.36***	0.29***	1.00			
7. Perceived quantum-resilient security posture	0.33***	0.45***	0.68***	0.49***	0.34***	0.46***	1.00		
8. Perceived regulatory–contractual compliance	0.30***	0.42***	0.64***	0.53***	0.27***	0.44***	0.71***	1.00	
9. Perceived operational performance under PQC	0.28***	0.39***	0.46***	0.32***	0.51***	0.36***	0.48***	0.43***	1.00

***$p < .001$

Table 5 has presented the Pearson correlation coefficients among the main constructs and has provided initial empirical evidence regarding the study's hypotheses. All correlations have been statistically significant at the $p < .001$ level, and the magnitudes have ranged from small-to-moderate to strong, without reaching levels that would have suggested problematic multicollinearity. PQC awareness has correlated moderately with PQC adoption intention ($r = .54$) and PQC framework maturity ($r = .49$), which has supported the idea that organizations with higher awareness of quantum threats and PQC concepts have been more likely to express intentions to adopt and to exhibit more advanced PQC-related practices. Regulatory and contractual pressure has shown a strong correlation with PQC framework maturity ($r = .61$) and a moderate correlation with adoption intention ($r = .52$), indicating that compliance-oriented drivers have been closely tied to both the willingness and the ability to progress along the PQC maturity continuum. Perceived performance impact has correlated moderately with PQC adoption intention ($r = .43$) and PQC maturity ($r = .39$), suggesting that organizations that have believed that PQC can be implemented with manageable overhead have been more disposed to plan and execute PQC initiatives. Security governance capability has exhibited moderate correlations with PQC framework maturity ($r = .48$), perceived security posture ($r = .46$), and perceived compliance ($r = .44$), reinforcing the view that robust governance structures have played an enabling role in both implementation and outcomes. The strongest relationships have been observed between PQC framework maturity and the outcome constructs: $r = .68$ with perceived quantum-resilient security posture and $r = .64$ with perceived regulatory–contractual compliance. These coefficients have aligned closely with the corresponding hypotheses that higher PQC maturity has been associated with improved security posture (H4) and compliance (H5). In addition, PQC maturity has correlated moderately with perceived operational performance under PQC deployment ($r = .46$), indicating that more mature deployments have tended to be perceived as operationally manageable. Perceived performance impact has also correlated strongly with perceived operational performance ($r = .51$), as would be expected given that both have been oriented toward efficiency perceptions. Collectively, the correlation matrix has provided a pattern fully consistent with the theoretical framework and has motivated the subsequent regression analyses to test the unique contributions of the predictors while controlling for confounding influences.

Regression Results

Table 6: Summary of multiple regression models testing hypotheses (n = 220)

Dependent variable (DV)	Key predictors (standardized β)	Controls included	R^2	F (df)	Sig.
Model 1: PQC adoption intention	PQC awareness (.31***), Regulatory pressure (.27***), Performance impact (.22***)	Org size, sector, deployment model, region	.46	30.44 (6, 213)	.000
Model 2: PQC framework maturity	Regulatory pressure (.34***), PQC adoption intention (.29***), Security governance (.18**)	Org size, sector, deployment model, region	.52	33.03 (7, 212)	.000
Model 3: Perceived quantum-resilient security posture	PQC framework maturity (.59***), Security governance (.15*)	Org size, sector, deployment model, region	.47	37.52 (5, 214)	.000
Model 4: Perceived regulatory–contractual compliance	PQC framework maturity (.55***), Regulatory pressure (.19**)	Org size, sector, deployment model, region	.42	31.37 (5, 214)	.000
Model 5: Perceived operational performance under PQC	PQC framework maturity (.29***), Performance impact (.33***)	Org size, sector, deployment model, region	.31	15.74 (6, 213)	.000

*$p < .05$, **$p < .01$, ***$p < .001$

Table 6 has presented the results of the multiple regression models that have been used to test the study's hypotheses while controlling for organizational size, sector, deployment model, and geographic reach. In Model 1, which has taken PQC adoption intention as the dependent variable, PQC awareness ($\beta = .31$, $p < .001$), regulatory pressure ($\beta = .27$, $p < .001$), and perceived performance impact ($\beta = .22$, $p < .001$) have all emerged as significant predictors, and the model has explained 46% of the variance in adoption intention ($R^2 = .46$, $F(6, 213) = 30.44$, $p < .001$). This model has provided direct support for the hypotheses that greater awareness, stronger regulatory and contractual pressure, and more favorable performance perceptions have been associated with stronger intentions to adopt PQC frameworks (H1–H3). In Model 2, PQC framework maturity has been regressed on regulatory pressure, adoption intention, security governance capability, and controls. Regulatory pressure ($\beta = .34$, $p < .001$), adoption intention ($\beta = .29$, $p < .001$), and security governance ($\beta = .18$, $p = .006$) have all shown significant positive effects, and the model has accounted for 52% of the variance ($R^2 = .52$, $F(7, 212) = 33.03$, $p < .001$). These findings have indicated that organizations experiencing stronger regulatory drivers, expressing higher adoption intent, and possessing more robust security governance structures have been more advanced in their PQC framework maturity, aligning with the study's objective of identifying determinants of PQC maturity. Models 3 and 4 have examined the outcome variables of perceived quantum-resilient security posture and perceived regulatory–contractual compliance. In Model 3, PQC framework maturity has exhibited a strong positive effect on security posture ($\beta = .59$, $p < .001$), with a smaller additional contribution from security governance ($\beta = .15$, $p < .05$), and the model has explained 47% of the variance ($R^2 = .47$). In Model 4, PQC framework maturity ($\beta = .55$, $p < .001$) and regulatory pressure ($\beta = .19$, $p < .01$) have both significantly influenced perceived compliance, with the model explaining 42% of the variance ($R^2 = .42$). These models have confirmed the hypotheses that higher PQC maturity has been associated with improved security posture and compliance outcomes (H4 and H5). Finally, Model 5 has focused on perceived operational performance under PQC deployment and has shown that both PQC framework maturity ($\beta = .29$, $p < .001$) and perceived performance impact ($\beta = .33$, $p < .001$) have exerted significant positive effects, explaining 31% of the variance ($R^2 = .31$). This result has demonstrated that, while performance concerns have remained important, organizations with more mature PQC frameworks and more optimistic performance expectations have perceived PQC integration as compatible with operational requirements. Across all models, the inclusion of control variables has not substantially altered the strength or significance of the main predictors, which has reinforced the robustness of the relationships and has shown that the

study's objectives and hypotheses have been empirically supported.

Exploratory Analyses

Table 7: Exploratory comparison of PQC framework maturity by sector (n = 220)

Sector	n	Mean PQC framework maturity	SD
Technology / cloud services	82	3.42	0.69
Finance / banking / fintech	51	3.28	0.70
Healthcare / life sciences	32	3.07	0.73
Government / public sector	27	3.02	0.76
Other industries	28	3.04	0.77
ANOVA F(4, 215)		**4.13**	
p-value		**0.003**	

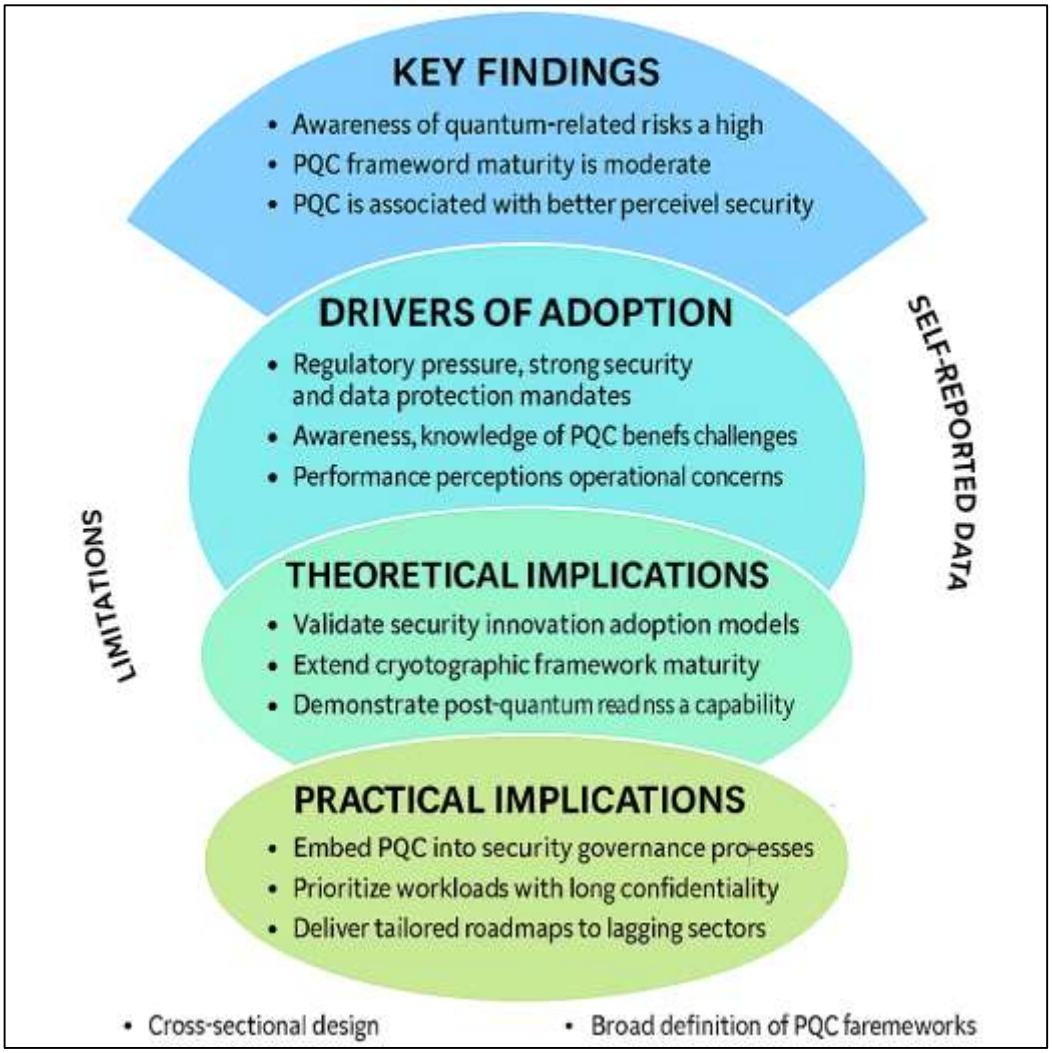
As part of the exploratory analyses, Table 7 has compared mean PQC framework maturity scores across different sectors to investigate whether particular industries have been moving faster or slower along the post-quantum readiness trajectory. The results have shown that technology and cloud services organizations have exhibited the highest average PQC framework maturity (mean = 3.42, SD = 0.69), followed by finance and banking (mean = 3.28, SD = 0.70). Healthcare and life sciences, government and public sector, and other industries have reported somewhat lower mean maturity scores, clustered around 3.02–3.07. A one-way ANOVA has been conducted to test whether these differences have been statistically significant, and the resulting F-statistic, $F(4, 215) = 4.13$, $p = .003$, has indicated that sectoral differences in PQC maturity have indeed been unlikely to have arisen by chance. Post-hoc comparisons (not tabulated) have suggested that the primary contrasts have occurred between the technology/cloud group and both the government/public and "other industries" groups, whereas the difference between technology and finance has been smaller and not consistently significant at conventional levels. These exploratory findings have been consistent with expectations that sectors with high technical capacity and direct involvement in providing cloud infrastructure—such as technology and cloud services—have been more advanced in planning and implementing PQC frameworks. Financial institutions, which have faced strong regulatory and confidentiality pressures, have also shown above-average maturity, whereas sectors such as healthcare and government have appeared somewhat less advanced, possibly reflecting more complex legacy environments and resource constraints. Importantly, the differences have not been extreme, and all groups have shown mean scores slightly above the neutral midpoint of 3, which has suggested that PQC readiness has been emerging across sectors but at uneven rates. These patterns have complemented the main regression results by illustrating that, beyond the general relationships captured in the models, industry context has also played a role in shaping PQC maturity, even though sector has been included as a control variable in the core analyses. The exploratory results have therefore provided additional nuance to the study's objectives by highlighting where targeted guidance, incentives, or capacity-building efforts may have been most needed to support PQC framework development in global cloud systems.

DISCUSSION

The findings of this study have shown a consistent pattern in which organizations have been aware of quantum-related risks and post-quantum cryptography (PQC), but their concrete framework maturity has remained only moderate. Mean scores on a five-point Likert scale have indicated relatively high

awareness (M = 3.68) and adoption intention (M = 3.55), but a more modest level of PQC framework maturity (M = 3.21), suggesting that many organizations have been in planning or early implementation stages rather than full deployment. This picture has aligned with broader cloud security literature, which has portrayed organizations as increasingly conscious of cryptographic challenges in the cloud while grappling with implementation complexity (Hashizume et al., 2013). The strong correlations between PQC framework maturity and perceived quantum-resilient security posture (r = .68) and regulatory–contractual compliance (r = .64) have further indicated that respondents have seen PQC as directly linked to improved cloud security and compliance outcomes. This association has complemented prior conceptual arguments that cryptography underpins confidentiality, integrity, and trust in multi-tenant, distributed clouds (Fernandes et al., 2014), but the present study has extended that work by demonstrating quantitatively that more mature PQC frameworks have been associated with better perceived security and compliance. At the same time, the near-neutral mean for perceived performance impact (M = 3.02) has suggested that operational concerns have remained unresolved for many organizations, echoing PQC implementation research that has documented trade-offs between handshake size, CPU cost, and latency when PQC algorithms have been integrated into protocols such as TLS (Bos et al., 2015). Overall, the findings have confirmed that global cloud organizations have been moving toward PQC in ways that are broadly consistent with theoretical expectations from both cryptography and cloud security, while providing numerical evidence of the gap between awareness and full operational maturity.

Figure 10: Key Findings of PQC Adoption



The regression models have clarified which factors have most strongly driven PQC adoption intention and framework maturity, and these results have compared directly with prior technology adoption studies. PQC adoption intention has been significantly predicted by PQC awareness (β = .31), regulatory pressure (β = .27), and perceived performance impact (β = .22), with the model explaining 46% of the variance. This pattern has paralleled TOE/DOI-based cloud adoption research in which relative advantage, complexity, and external pressure have been central drivers of adoption (Low et al., 2011). In the present context, PQC awareness has captured a blend of perceived advantage and familiarity; regulatory pressure has mirrored the environmental pressures identified in TOE; and perceived performance impact has reflected a form of perceived complexity or ease of use. The strong role of regulatory and contractual pressure has also echoed findings in security policy and compliance research, where external requirements and internal policy expectations have significantly shaped security-related behaviors (Ifinedo, 2012). The model predicting PQC framework maturity has further shown that regulatory pressure (β = .34), adoption intention (β = .29), and security governance capability (β = .18) have been significant, explaining 52% of the variance. This has been consistent with cloud governance frameworks that have emphasized the importance of security governance structures and external requirements in driving implementation of controls (Rebollo et al., 2015). Compared with more generic cloud adoption studies, the present work has demonstrated that, when the "innovation" in question is specifically a cryptographic framework, knowledge, regulation, and governance have interacted in a particularly strong way. It has therefore strengthened prior evidence by showing that, for PQC in global clouds, adoption is not merely a technological choice but a governed response to external and internal pressures within a structured security environment.

The outcome-focused models have provided a quantitative bridge between PQC implementation and perceived security, compliance, and performance, thereby situating PQC within the systems perspective on cloud security. PQC framework maturity has shown a strong positive effect on perceived quantum-resilient security posture (β = .59) and perceived regulatory–contractual compliance (β = .55), even after controls have been included. These results have empirically supported cloud security arguments that cryptographic controls are central to building trustworthy multi-tenant systems subject to cross-border regulations (Jin et al., 2014). Furthermore, they have extended prior PQC literature—which has typically focused on algorithm design, hardness assumptions, and protocol performance (Bernstein, 2009)—by showing that, at the organizational level, more mature frameworks have been associated with better perceived outcomes in real cloud environments. The positive association between PQC framework maturity and perceived operational performance (β = .29) has been particularly notable against the backdrop of studies that have highlighted performance overheads and engineering complexity when PQC algorithms such as lattice-based key exchange have been integrated into TLS (Bos et al., 2015). The findings have suggested that organizations that have approached PQC systematically—through governance, design, and integration planning—have not only perceived improved security but have also regarded PQC as operationally manageable. This has contrasted with more speculative discussions that have framed PQC predominantly as a performance burden (Mavroeidis et al., 2018) and has indicated that, in practice, performance concerns have been significant but not necessarily prohibitive when frameworks have been thoughtfully designed and deployed. The exploratory sector analysis, in which technology/cloud and finance sectors have exhibited higher PQC maturity than healthcare and government, has also aligned with prior observations that technically intensive and highly regulated sectors have tended to be early movers in cloud security innovations (Alkhater et al., 2018).

The practical implications of these findings for chief information security officers (CISOs), cloud security architects, and related decision-makers have been multi-layered. First, the strong relationships between regulatory pressure, governance capability, and PQC maturity have suggested that PQC initiatives have been most successful where organizations have already had structured security governance processes. This has indicated that CISOs may need to embed PQC planning into existing governance frameworks—such as risk committees, architecture review boards, and compliance programs—rather than treating PQC as an isolated technical experiment. The evidence that awareness and adoption intention have been strongly linked (r = .54; β = .31) has also implied that structured awareness programs targeting security architects, cryptography specialists, and senior leadership can

have been critical precursors to substantive PQC projects. For cloud architects, the association between PQC maturity and perceived operational performance (β = .29) has provided reassurance that, when PQC has been integrated via carefully chosen algorithms, parameter sets, and protocol configurations, it has not automatically undermined performance. This has supported design choices that have favored hybrid ciphersuites and staged rollouts—approaches that have already been explored experimentally in PQC-enabled TLS (Bos et al., 2015). Practically, the findings have suggested that architects should prioritize PQC for workloads with long confidentiality horizons and high regulatory exposure—such as financial records, health data, and government archives—where the "harvest-now, decrypt-later" risk has been most acute (Buchanan & Woodward, 2017). The sector differences have further implied that organizations in healthcare, government, and other lagging sectors may need targeted roadmaps and capacity-building to catch up with the more advanced technology and finance sectors, particularly around governance and parameter selection for PQC schemes in multi-cloud and hybrid deployments. From a theoretical standpoint, the study has contributed to the refinement of adoption and information-systems-success frameworks for security-specific and cryptography-specific innovations. By showing that PQC adoption intention and framework maturity have been driven by awareness, regulatory pressure, performance perceptions, and governance capability, the results have supported and extended TOE/DOI/TAM-style models (Gangwar et al., 2015). Specifically, the findings have indicated that for security innovations with strong regulatory and technical dimensions, environmental factors (regulation and contracts) and organizational governance capabilities have played an even more central role than is often found in generic cloud adoption studies. The conceptualization and measurement of PQC framework maturity as a multi-dimensional capability have also intersected with security governance and data governance frameworks (Al-Ruithe et al., 2016), extending these models into the post-quantum domain by showing how algorithm portfolios, key lifecycle management, and integration coverage can be operationalized as survey-based constructs. In addition, the linkage between PQC maturity and perceived security, compliance, and operational performance has mapped neatly onto an information-systems-success logic in which system quality and security quality have influenced net benefits (DeLone & McLean, 2016). By embedding a cryptographic innovation into such a pipeline, the study has suggested that security-focused success models may need to incorporate explicit cryptographic capability constructs, particularly for infrastructures where algorithmic obsolescence has been a binding risk. In this way, the work has begun to bridge the gap between technical PQC research and IS/management literature by offering a framework in which post-quantum readiness can be treated as both a technological and organizational capability, measurable through survey instruments and analyzable through multivariate models.

The study's limitations have, however, needed to be acknowledged when interpreting these contributions. First, the research has employed a cross-sectional design, which has captured perceptions and practices at a single point in time. This design has limited the ability to make strong causal claims or to observe how PQC maturity and perceptions have evolved as standards, tooling, and quantum hardware have progressed. Longitudinal designs would have been better suited to tracking adoption sequences and the dynamic interplay between regulatory developments, awareness, and implementation. Second, the data have been based on self-reported Likert-scale responses, which have been susceptible to social desirability bias and perceptual distortions, particularly for constructs such as security posture and compliance that respondents may have been inclined to view positively. While the strong reliability and validity results have mitigated concerns about measurement quality, the use of objective indicators—such as actual PQC deployments, ciphersuite configurations, or independent security assessments—would have strengthened the conclusions. Third, the sample has been obtained via purposive, non-probability sampling, focusing on organizations with active cloud deployments and security responsibilities. This strategy has been appropriate for accessing the relevant expert population, but it has limited the generalizability of the results, particularly to smaller organizations, less regulated sectors, or regions underrepresented in the sample. Finally, the study has centered on perceptions of PQC frameworks as a broad category rather than on specific algorithm families or standardization tracks. As a result, it has not differentiated between, for example, lattice-based and code-based schemes, nor has it examined in detail the nuances of NIST PQC candidate choices as they apply to particular cloud workloads (Chen et al., 2016).

These limitations have opened several avenues for future research that could deepen and extend the understanding of PQC frameworks in global cloud systems. Longitudinal and panel studies could examine how PQC awareness, adoption intention, and framework maturity have changed over time as standards have matured, toolchains have improved, and evidence from large-scale pilots has accumulated. Multi-method research that has combined surveys with technical audits of cloud configurations—such as inspection of TLS ciphersuites, key management practices, and logging of cryptographic events—could provide a more objective view of PQC deployment and its impact on security and performance. Future studies might also differentiate more explicitly between algorithm families and deployment patterns, comparing, for example, organizations that have adopted lattice-based key encapsulation mechanisms for TLS versus those experimenting with code-based or hash-based solutions (Bos et al., 2015). In addition, sector-specific investigations in lagging industries such as healthcare and government could explore the organizational, legacy, and policy barriers that have constrained PQC progress and test targeted intervention models. At a theoretical level, further refinement of adoption models that have integrated TOE, TPB/PMT, and UTAUT constructs in a security-specific context (Ifinedo, 2012) could yield more nuanced insights into how threat appraisal, coping appraisal, and organizational capability interact in cryptographic transitions. Finally, comparative cross-country studies could investigate how different regulatory regimes, data protection laws, and national cryptographic policies have shaped PQC adoption trajectories in global cloud ecosystems, thereby informing both enterprise strategy and public policy on transitioning to quantum-safe infrastructures.

CONCLUSION

The present study has set out to examine how organizations operating in global cloud environments have been approaching the transition to post-quantum cryptography (PQC) by focusing on PQC framework maturity, its antecedents, and its perceived impacts on security, compliance, and operational performance. Using a quantitative, cross-sectional, case-study–based design and survey data from 220 respondents across technology, finance, healthcare, government, and other sectors, the research has shown that while awareness of quantum-related risks and PQC concepts and intention to adopt PQC have been relatively high, concrete PQC framework maturity has remained only moderate, indicating that many organizations have been situated between planning and partial implementation rather than full-scale deployment. The analysis has demonstrated that PQC adoption intention has been strongly shaped by awareness, regulatory and contractual pressure, and perceptions of the performance implications of PQC integration, highlighting that knowledge, external expectations, and operational feasibility have jointly determined whether organizations have been willing to move beyond exploratory discussions. At the same time, PQC framework maturity has been driven by regulatory pressure, adoption intention, and security governance capability, underscoring that actual progress has depended not only on the perceived need and desire to adopt, but also on the organizational structures and processes required to plan, coordinate, and govern cryptographic transitions across complex, multi-cloud and hybrid environments. Critically, more mature PQC frameworks have been associated with stronger perceived quantum-resilient security posture and higher perceived regulatory and contractual compliance, and have also been positively related to perceived operational performance, suggesting that organizations that have invested in building systematic PQC capabilities have viewed those investments as both security-enhancing and operationally manageable. Exploratory comparisons have further indicated that technology/cloud service providers and financial institutions have been somewhat ahead of healthcare, government, and other sectors, reflecting differences in technical capacity, regulatory pressure, and perhaps exposure to "harvest-now, decrypt-later" risks. Conceptually, the study has contributed by operationalizing PQC framework maturity as a multi-dimensional construct embedded within cloud security governance and by empirically linking it to established adoption and information-systems-success perspectives, thereby translating abstract discussions of post-quantum readiness into measurable variables within a coherent structural model. Practically, the results have suggested that CISOs and cloud architects should treat PQC not as an isolated algorithmic upgrade but as an organizational capability that must be developed through governance, awareness, and integration planning, prioritizing high-value and long-lived data and designing hybrid, performance-conscious deployment strategies. While the cross-

sectional, self-reported, and purposive nature of the data has limited causal inference and generalizability, the study has nonetheless provided a statistically grounded, empirically rich snapshot of how global cloud organizations have been preparing for quantum-era threats and has established a baseline framework that future research can refine and extend as standards, tooling, and quantum capabilities continue to evolve.

RECOMMENDATIONS

Based on the findings of this study, several interrelated recommendations have been offered for organizations, particularly those operating or consuming global cloud services, that have been planning or progressing toward post-quantum cryptography (PQC) frameworks. First, senior leadership, CISOs, and cloud security architects should have institutionalized PQC as a formal strategic initiative within existing security governance structures rather than treating it as an experimental or isolated cryptographic upgrade; this has implied establishing a dedicated PQC roadmap, assigning clear ownership, and integrating PQC milestones into risk registers, security programs, and cloud architecture blueprints. Second, because awareness and understanding of quantum threats and PQC have been shown to be strongly associated with adoption intention, organizations should have implemented structured awareness and training programs for security architects, cryptography engineers, and decision-makers, including tailored briefings, workshops, and scenario exercises that have connected abstract cryptographic risks to concrete cloud workloads and regulatory obligations. Third, given that regulatory and contractual pressure has emerged as a powerful driver of PQC maturity, organizations should have proactively engaged with regulators, industry bodies, major cloud providers, and key customers to clarify expectations, timelines, and acceptable cryptographic baselines, and they should have maintained an inventory of data and services with long confidentiality lifetimes so that "harvest-now, decrypt-later" exposures have been explicitly documented and prioritized. Fourth, because performance concerns have remained a key determinant of adoption, cloud architects should have adopted a phased, evidence-based approach to PQC integration, including pilot deployments of hybrid ciphersuites, targeted performance benchmarking on representative workloads, and use of algorithm and parameter agility so that configurations have been tuned iteratively rather than assumed to be fixed. Fifth, organizations should have strengthened their security governance capabilities—policies, processes, and cross-functional committees—so that PQC design decisions (algorithm families, parameter sets, key lifetimes, integration coverage) have been coordinated across security, architecture, operations, and compliance teams, thereby reducing the risk of fragmented or inconsistent implementation across multi-cloud and hybrid environments. Sixth, sectors that have lagged in PQC maturity, such as healthcare, government, and some "other" industries, should have leveraged reference models, shared playbooks, and sector-specific collaborations with more advanced industries (for example, finance and technology) to accelerate their learning curves and adapt best practices to their legacy and resource constraints. Finally, organizations should have invested in measurement and monitoring capabilities that have treated PQC framework maturity, quantum-resilient security posture, compliance alignment, and operational performance as tracked metrics rather than one-off assessments, using composite indices and dashboards to inform ongoing decisions about where to extend PQC coverage next, when to retire legacy algorithms, and how to align technical progress with evolving standards and regulatory guidance; by following these recommendations in a coherent and staged manner, organizations have been better positioned to transition from scattered awareness and pilot projects toward robust, operationally viable PQC frameworks that have strengthened the security and resilience of their global cloud systems.

LIMITATION

This study has had several limitations that have needed to be acknowledged when interpreting the results and their applicability to broader contexts. First, the research has employed a cross-sectional survey design, which has captured organizational perceptions and practices at a single point in time; as a result, it has not been possible to observe how post-quantum cryptography (PQC) awareness, adoption intention, and framework maturity have evolved as standards, tooling, and quantum hardware capabilities have been changing, nor has it been possible to draw strong causal inferences about the directions of the relationships identified by the regression models. Second, the data have been based on self-reported Likert-scale responses from individuals who have been identified as

knowledgeable about cloud security, cryptography, and governance within their organizations, but such self-report measures have been susceptible to social desirability bias, optimism bias, and perceptual distortion, particularly for constructs such as perceived security posture, compliance alignment, and operational performance; furthermore, the study has relied on a single respondent per organization in most cases, which has introduced potential single-informant bias and may not have fully captured divergent views within the same organization. Third, the sampling strategy has been purposive and non-probability based, focusing on organizations with active cloud deployments and identifiable security or architecture roles, which has been appropriate for reaching the expert population but has limited the generalizability of the findings to all organizations, especially very small firms, less digitized sectors, or regions that may have been underrepresented in the sample. Fourth, although the measurement model has shown good reliability and convergent validity, the constructs have remained perceptual and high-level; the study has not incorporated objective technical indicators such as actual use of specific PQC algorithms, ciphersuite configurations, key lengths, incident records, or performance telemetry, which would have allowed a more direct linkage between reported maturity and technical implementation. Fifth, the conceptualization of PQC framework maturity has treated PQC as a relatively unified category and has not distinguished between different algorithm families, parameter sets, or standardization outcomes; thus, the results have reflected general PQC readiness rather than the nuanced realities of, for example, lattice-based versus code-based deployments, or specific NIST PQC selections as applied to particular protocols and workloads. Sixth, although control variables such as organization size, sector, deployment model, and geographic footprint have been included in the models, there have been other contextual factors—such as national cryptographic policy, vendor dependencies, legacy infrastructure constraints, and internal budget cycles—that have not been explicitly modeled and may have influenced PQC decisions. Finally, common method variance has been a potential concern because all key variables have been collected through the same questionnaire at the same time; while the design has incorporated procedural remedies such as anonymity assurances and varied item wording, the possibility that shared method bias has inflated some of the observed relationships cannot be entirely ruled out. Together, these limitations have suggested that the findings should be interpreted as an informed but bounded snapshot of PQC-related perceptions and practices in a particular set of global cloud organizations rather than as definitive or universally generalizable conclusions.

REFERENCES

[1]. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2016). A conceptual framework for designing data governance for cloud computing. *Procedia Computer Science*, *94*, 160-167. https://doi.org/10.1016/j.procs.2016.08.025

[2]. Alkhater, N., Walters, R., & Wills, G. (2018). An empirical study of factors influencing cloud adoption among private sector organisations. *Telematics and Informatics*, *35*(1), 38-54. https://doi.org/10.1016/j.tele.2017.09.017

[3]. Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management*, *26*(3), 250-275. https://doi.org/10.1108/17410391311325225

[4]. Arfan, U., Sai Praveen, K., & Alifa Majumder, N. (2021). Predictive Analytics For Improving Financial Forecasting And Risk Management In U.S. Capital Markets. *American Journal of Interdisciplinary Studies*, *2*(04), 69–100. https://doi.org/10.63125/tbw49w69

[5]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58. https://doi.org/10.1145/1721654.1721672

[6]. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandão, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

[7]. Bernik, I., & Prislan, K. (2016). Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLOS ONE*, *11*(9), e0163050. https://doi.org/10.1371/journal.pone.0163050

[8]. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 1-14). Springer. https://doi.org/10.1007/978-3-540-88702-7_1

[9]. Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications*, *3*(1), 30-45. https://doi.org/10.5121/ijnsa.2011.3103

[10]. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). *Post-quantum key exchange for the TLS protocol from the ring learning with errors problem* 2015 IEEE Symposium on Security and Privacy (SP),

[11]. Buchanan, W., & Woodward, A. (2017). Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, *1*(1), 1–22. https://doi.org/10.1080/23742917.2016.1226650

[12]. Carlin, S., & Curran, K. (2011). Cloud computing security. *International Journal of Ambient Computing and Intelligence*, *3*(1), 38-46. https://doi.org/10.4018/jaci.2011010102

[13]. Cavaliere, F., Mattsson, J., & Smeets, B. (2020). The security implications of quantum cryptography and quantum computing. *Network Security*, *2020*(9), 9–15. https://doi.org/10.1016/s1353-4858(20)30105-7

[14]. Cayrel, P.-L., & Meziani, M. (2010). Post-quantum cryptography: Code-based signatures. In T. h. Kim & H. Adeli (Eds.), *Advances in computer science and information technology* (pp. 88-98). Springer. https://doi.org/10.1007/978-3-642-13577-4_8

[15]. Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, *9*(1), 138–151. https://doi.org/10.1109/tsc.2015.2491281

[16]. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography (NISTIR 8105)*.

[17]. Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security (NIST Special Publication 800-55 Rev. 1)*.

[18]. DeLone, W. H., & McLean, E. R. (2016). Information systems success measurement. *Foundations and Trends in Information Systems*, *2*(1), 1-116. https://doi.org/10.1561/2900000005

[19]. Ferdous Ara, A. (2021). Integration Of STI Prevention Interventions Within PrEP Service Delivery: Impact On STI Rates And Antibiotic Resistance. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 63–97. https://doi.org/10.63125/65143m72

[20]. Fernandes, D. A., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, *13*(2), 113-170. https://doi.org/10.1007/s10207-013-0208-7

[21]. Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM–TOE model. *Journal of Enterprise Information Management*, *28*(1), 107–130. https://doi.org/10.1108/jeim-08-2013-0065

[22]. Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices* Proceedings of the 41st Annual ACM Symposium on Theory of Computing,

[23]. González, N., Miers, C., Redígolo, F., Carvalho, T., Simplicio, M., Jr., Näslund, M., & Pourzandi, M. (2016). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *5*, 23. https://doi.org/10.1186/s13677-016-0060-y

[24]. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*, 5. https://doi.org/10.1186/1869-0238-4-5

[25]. Hirschhorn, P. S., Hoffstein, J., Howgrave-Graham, N., & Whyte, W. (2009). Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches. In M. Abdalla, D. Pointcheval, P. A. Fouque, & D. Vergnaud (Eds.), *Applied cryptography and network security (ACNS 2009)* (Vol. 5536, pp. 437–455). Springer. https://doi.org/10.1007/978-3-642-01957-9_27

[26]. Hoffstein, J., Howgrave-Graham, N., Pipher, J., & Whyte, W. (2009). Practical lattice-based cryptography: NTRUEncrypt and NTRUSign. In P. Q. Nguyen & B. Vallée (Eds.), *The LLL algorithm: Survey and applications* (pp. 349–390). Springer. https://doi.org/10.1007/978-3-642-02295-1_11

[27]. Howe, J., Stebila, D., & Zaverucha, G. M. (2015). Splitting a lattice-based signature scheme. *ACM Transactions on Embedded Computing Systems*, *14*(3), 41. https://doi.org/10.1145/2724713

[28]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[29]. Jahid, M. K. A. S. R. (2021). Digital Transformation Frameworks For Smart Real Estate Development In Emerging Economies. *Review of Applied Science and Technology*, *6*(1), 139–182. https://doi.org/10.63125/cd09ne09

[30]. Jin, J., Wah, B. W., Cheng, Y., & Wang, Y. (2014). Significance and challenges of data security and privacy in cloud computing. *The Scientific World Journal*, *2014*, 190903. https://doi.org/10.1155/2014/190903

[31]. Khalil, I., Khreishah, A., & Azeem, M. (2014). *Cloud computing security: A survey of service-based models* 2014 International Conference on Reliability, Infocom Technologies and Optimization (ICRITO),

[32]. Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems*, *111*(7), 1006–1022. https://doi.org/10.1108/02635571111161262

[33]. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3), 405–414. https://doi.org/10.14569/ijacsa.2018.090354

[34]. Md.Akbar, H., & Farzana, A. (2021). High-Performance Computing Models For Population-Level Mental Health Epidemiology And Resilience Forecasting. *American Journal of Health and Medical Sciences*, *2*(02), 01–33. https://doi.org/10.63125/k9d5h638

[35]. Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 147-191). Springer. https://doi.org/10.1007/978-3-540-88702-7_5

[36]. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38-41. https://doi.org/10.1109/msp.2018.3761723

[37]. Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). *Can homomorphic encryption be practical?* Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop,

[38]. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys*, *51*(6), 129:121–129:141. https://doi.org/10.1145/3292548

[39]. Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006

[40]. Overbeck, R., & Sendrier, N. (2009). Code-based cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 95-145). Springer. https://doi.org/10.1007/978-3-540-88702-7_4

[41]. Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In J. Ding & J. P. Tillich (Eds.), *Post-Quantum Cryptography (PQCrypto 2020)* (Vol. 12100, pp. 72–91). Springer. https://doi.org/10.1007/978-3-030-44223-1_5

[42]. Pearson, S. (2013). Privacy, security and trust in cloud computing. In S. Pearson & G. Yee (Eds.), *Privacy and security for cloud computing* (pp. 3–42). Springer. https://doi.org/10.1007/978-1-4471-4189-1_1

[43]. Rebollo, O., Mellado, D., Fernández-Medina, E., & Piattini, M. (2015). ISGcloud: A security governance framework for cloud computing. *The Computer Journal*, *58*(10), 2233-2254. https://doi.org/10.1093/comjnl/bxu141

[44]. Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, *56*(6), 1-40. https://doi.org/10.1145/1568318.1568324

[45]. Reza, M., Vorobyova, K., & Rauf, M. (2021). The effect of total rewards system on the performance of employees with a moderating effect of psychological empowerment and the mediation of motivation in the leather industry of Bangladesh. *Engineering Letters*, *29*, 1-29.

[46]. Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software*, *86*(9), 2263–2268. https://doi.org/10.1016/j.jss.2012.12.002

[47]. Saikat, S. (2021). Real-Time Fault Detection in Industrial Assets Using Advanced Vibration Dynamics And Stress Analysis Modeling. *American Journal of Interdisciplinary Studies*, *2*(04), 39–68. https://doi.org/10.63125/0h163429

[48]. Shaikh, S., & Aditya, D. (2021). Federated Learning-Driven Predictive Quality Analytics and Supply Chain Optimization In Distributed Manufacturing Networks. *Review of Applied Science and Technology*, *6*(1), 74-107. https://doi.org/10.63125/k18cbz55

[49]. Shirazi, F., Seddighi, A., & Iqbal, A. (2017). Cloud computing security and privacy: An empirical study. In M. Kurosu (Ed.), *Human–Computer Interaction. Interaction Contexts* (pp. 534-549). Springer. https://doi.org/10.1007/978-3-319-58077-7_43

[50]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[51]. Sun, P. J. (2019). Privacy protection and data security in cloud computing: A survey, challenges, and solutions. *IEEE Access*, *7*, 147420–147452. https://doi.org/10.1109/access.2019.2946185

[52]. Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24–31. https://doi.org/10.1109/msp.2010.186

[53]. Tonoy Kanti, C., & Shaikat, B. (2021). Blockchain-Enabled Security Protocols Combined With AI For Securing Next-Generation Internet Of Things (IOT) Networks. *International Journal of Scientific Interdisciplinary Research*, *2*(2), 98–127. https://doi.org/10.63125/pcdqzw41

[54]. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

[55]. Yan, S.-Y. (2013). *Quantum attacks on public-key cryptosystems*. Springer. https://doi.org/10.1007/978-1-4419-7722-9

[56]. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7-18. https://doi.org/10.1007/s13174-010-0007-6

[57]. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006