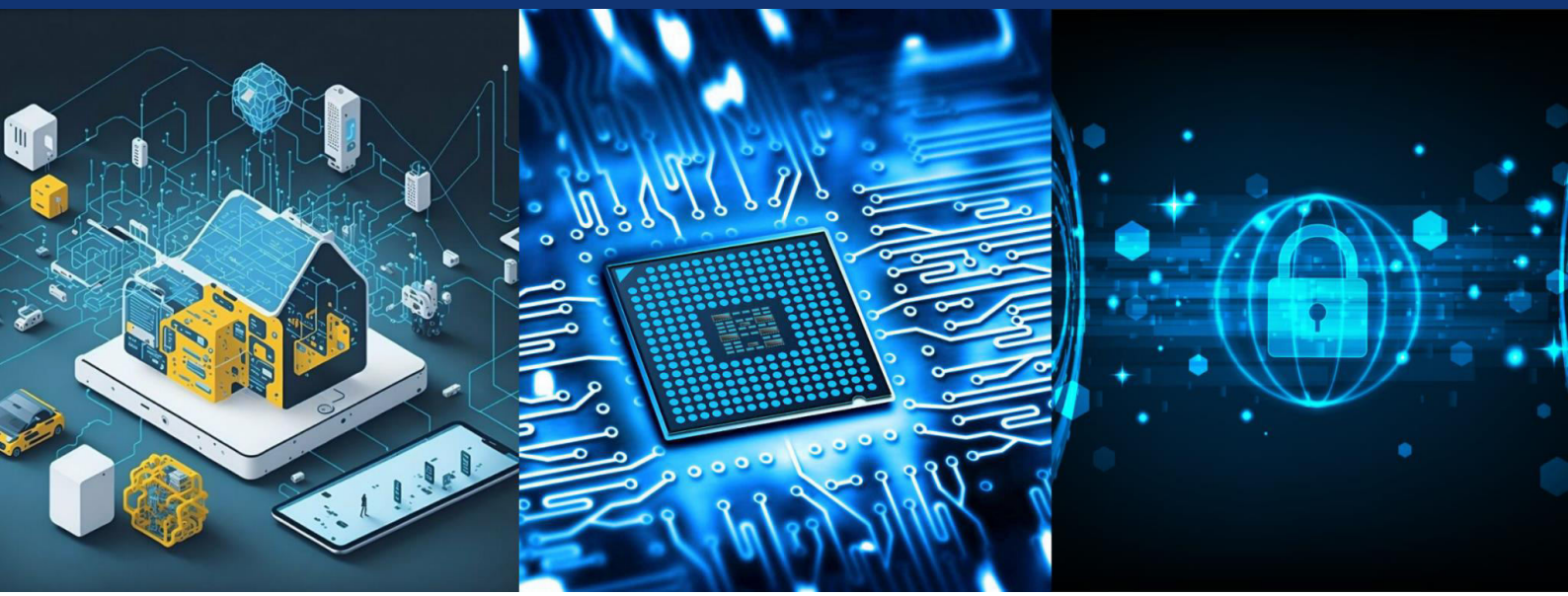
IJIRCCE

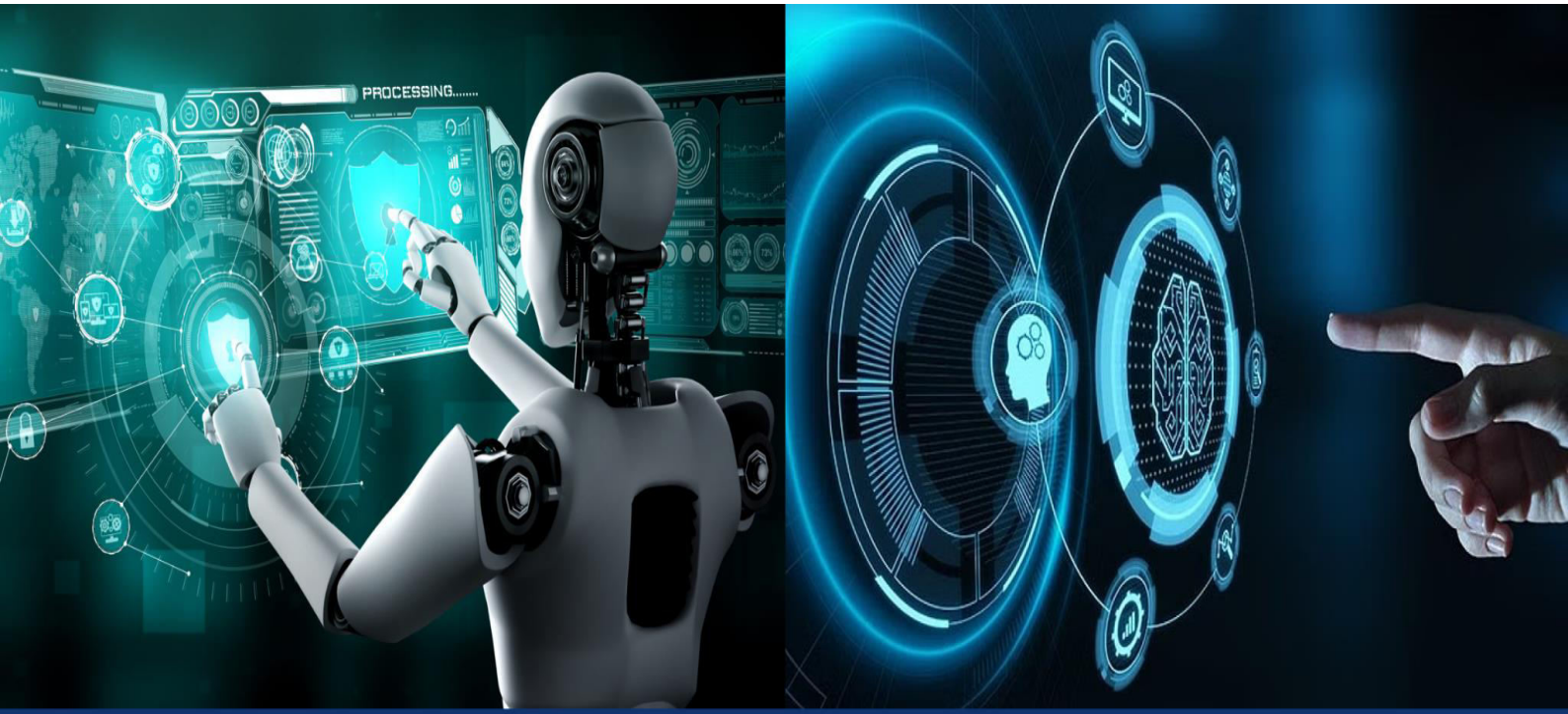
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 10, October 2026

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Quantum-Resistant Access Control System with Efficient Revocation for Cloud

C.M.S.Dhanushri, K.N.Sivakumar, S.Dinesh Kumar

Research Scholar, Department of Computer Science and Engineering, M.P.Nachimuthu M.Jaganathan Engineering College (An Autonomous Institution), Chennimalai, Erode, India

Associate Professor & Head, Department of Computer Science and Engineering, M.P.Nachimuthu M.Jaganathan Engineering College (An Autonomous Institution), Chennimalai, Erode, India

Department of Computer Science and Engineering, M.P.Nachimuthu M.Jaganathan Engineering College (An Autonomous Institution), Chennimalai, Erode, India

ABSTRACT: The proliferation of Internet of Things (IoT) devices in cloud-assisted environments raises urgent concerns regarding fine-grained access control, policy privacy, and resilience against quantum adversaries. To address these challenges, we propose a lightweight and quantum-resistant access control framework that combines Ring-LWE-based Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with fog-assisted split-path partial encryption architecture. In our scheme, IoT devices encrypt raw data using AES-256-GCM, while fog nodes perform the RLWE-CP-ABE encapsulation of session keys, thereby reducing device-side computation while ensuring that neither plaintext nor session keys are exposed to semi-trusted fog nodes. To preserve policy confidentiality, we integrate a salted attribute-hashing mechanism into the Linear Secret Sharing Scheme (LSSS) matrices, concealing access policies even during fog-side processing. Furthermore, we design an epoch-based and blacklist-based revocation mechanism that supports both user-level and attribute-level revocation without requiring ciphertext re-encryption. Security is guaranteed through CRYSTALS-Dilithium signatures and Poly1305 message authentication, which provide post-quantum authenticity and integrity. Experimental results confirm that our framework significantly reduces computational and communication overhead while achieving scalable, verifiable, and post-quantum-secure access control outperforming existing lattice-based CP-ABE schemes in both efficiency and security.

KEYWORDS: Multi-Authority, Revocation, Outsourced Decryption, Forward Security, Cloud Security.

I. INTRODUCTION

Quantum Computing (QC) has evolved from theory into a technological force threatening contemporary cryptographic systems. Enabled by quantum mechanical phenomena such as superposition and entanglement, QC offers exponential speedups for solving problems considered intractable for classical computers [1]. Critically, advances in quantum hardware threaten the foundational pillars of modern security, including RSA, DHE, and ECC, by exploiting their underlying mathematical hardness via Shor's [2] and Grover's [3] algorithms. The implications for Cloud Computing (CC) security are profound. Cloud infrastructures process vast quantities of sensitive data, from personal information and financial records to critical infrastructure controls, across extensively virtualized, containerized, and distributed microservices architectures.

As illustrated in Figure 1, CC is inherently multilayered, spanning application services to networking, with each layer presenting distinct security challenges. These layers underpin Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models, each defining distinct user and provider responsibility boundaries [11]. This complexity necessitates systematic, layer-specific risk analysis, as quantum vulnerabilities manifest differently across service models.

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

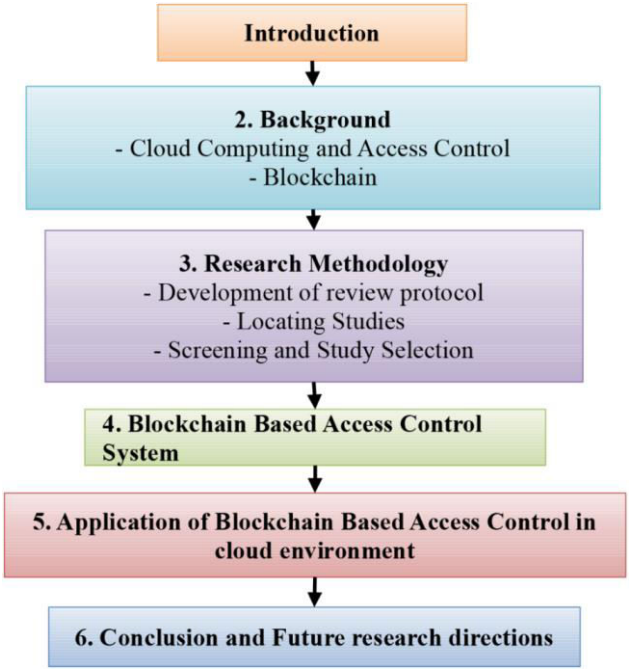


Fig 1: access control systems in cloud environment

CSP security/posture analysis of AWS, Azure, and GCP. Third, we propose a layered mitigation strategy spanning pre-quantum exposure, hybrid cryptographic deployment, and post-quantum hardening, covering defense-in-depth, cryptoagility, and fault/intrusion tolerance. Fourth, we provide actionable guidance and deployment blueprints for CSPs, auditors, and enterprise users. Finally, we introduce a hybrid cryptographic transition orchestration model that balances robustness with compatibility and operational continuity. This contrasts with prior works that remain conceptual or fragmented, as summarized.

With the rapid advancement of cloud computing and the Internet of Things (IoT), massive data outsourcing has become an inevitable trend. However, this paradigm brings significant challenges to data security and fine-grained access control. Traditional single-authority Attribute-Based Encryption (ABE) schemes suffer from inherent drawbacks such as key escrow, heavy computational overhead, and inefficient user revocation. To overcome these limitations, this paper presents an efficient Multi-Authority Revocable Attribute-Based Encryption (MA-RABE) scheme. The proposed scheme eliminates the need for a centralized authority by employing a distributed key generation protocol, ensuring secure and decentralized master key distribution while mitigating single points of failure. Furthermore, a lightweight attribute revocation mechanism is designed, which only requires updating the user's attribute key and one ciphertext component, significantly reducing computation and communication costs. To guarantee forward security, a version-based revocation strategy is introduced to prevent revoked users from decrypting previously accessible ciphertexts. In addition, the scheme supports outsourced decryption, allowing computationally intensive operations to be executed by a semi-trusted server, thereby minimizing local computational load on end devices. Security analysis shows that the proposed scheme achieves IND-CPA security and resists collusion attacks, while performance evaluation demonstrates that it achieves lower computational overhead in key generation, encryption, and decryption compared with existing approaches. Hence, the scheme is particularly suitable for resource-constrained mobile and IoT environments.

II. RELATED WORK

Prior literature on quantum-era cloud security clusters into three strands: (i) vulnerability-centric studies that catalog weaknesses without formal, NIST-aligned risk modeling or CSP-specific guidance [14], [16], [17]; (ii) quantum/architecture works outlining integration patterns but offering neither evidence of NIST-standard PQC adoption nor hybrid cryptographic migration orchestration [15], [18]; and (iii) attack-taxonomy surveys mapping threats yet lacking implementation-level roadmaps and post-migration hardening [19]. Across these strands, we observe

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

consistent gaps in (a) STRIDE-based, NIST-aligned cloud risk assessment; (b) CSP security/posture analysis for AWS, Azure, and GCP; (c) governance-aware hybrid transition planning; and (d) postmigration assurance.

Our work addresses these gaps by presenting a technically rigorous, multi-dimensional framework. First, we operationalize a NIST-aligned risk model using STRIDE and likelihood–impact evaluation to prioritize quantum-era threats across the cloud stack. Second, we conduct a granular We adopted a structured multi-stage review methodology spanning PQC, layered cloud architectures, threat modeling, and CSP quantum-safe migration strategies. Studies were included if they addressed: (a) quantum vulnerabilities across transition stages; (b) formal threat modeling frameworks (STRIDE, NIST SP 800-30); (c) hybrid cryptographic migration; (d) NIST PQC candidate evaluation; or (e) CSP quantum readiness initiatives. Studies lacking cloud specificity or formal modeling were excluded. We searched IEEE Xplore, ACM Digital Library, SpringerLink, Scopus, arXiv, PQCrypto/CRYPTO/EUROCRYPT proceedings, top journals (ACM Computing Surveys, IEEE Communications Surveys & Tutorials, IEEE TIFS, Journal of Cryptology), and CSP technical documentation. Search queries targeted PQC adoption, cloud-layer security, quantum threats, and migration strategies, yielding 15,000 initial records. After duplicate removal and screening, 200+ studies were mapped to our ninelayer architecture (Figure 1), classified by transition phase relevance (Sections IV, V), aligned with STRIDE and NIST SP 800-30, and analyzed for CSP quantum-safe deployment strategies.

Section II presents structured risk assessment methodology to evaluate quantumspecific threats during cloud migration. Section III examines classical cryptographic vulnerabilities exposed by QC and emerging PQC risks. Sections IV and V analyze threat landscapes across cloud layers, contrasting pre-transition vulnerabilities with quantum security postures. Section VI explores hybrid deployment strategies enabling phased, backwardcompatible quantum-safe adoption. Section VII benchmarks NIST-standardized PQC algorithms, evaluating computational efficiency and cloud deployment suitability. Section VIII presents comparative analysis of quantum-resistant implementations by major cloud providers, examining their technical approaches and capabilities. Section IX identifies research priorities in standardization, scalability, and emerging technology integration. Section X synthesizes key insights and provides actionable recommendations for strengthening cloud infrastructure resilience against quantum-era threats.

III. METHODS

We establish assessment scope through purpose, boundaries, assumptions, and threat models for systematic risk identification across transition stages. Our threat model assumes adversaries possess quantum resources to execute Shor's and Grover's algorithms, while accounting for current PQC limitations in efficiency, interoperability, and implementation readiness. We employ STRIDE-based threat categorization [24], [25] with discrete likelihood-impact criteria (Low, Medium, Risk assessment comprises five tasks: (1) identifying threat sources and events, (2) identifying vulnerabilities, (3) determining likelihood, (4) determining impact, and (5) assessing risk. Figure 3 summarizes this process.

We identify quantum-specific threats across three transition phases: (a) pretransition threats target classical cryptography (e.g., Shor's and Grover's algorithms breaking RSA, ECC, symmetric encryption); (b) transition threats exploit hybrid implementation weaknesses (e.g., downgrade attacks, protocol misconfigurations, PQC side-channel vulnerabilities); (c) post-transition threats target quantum-resistant systems via implementation flaws and advanced vectors (e.g., fault injection, quantumenhanced side-channel attacks). These adversaries exploit vulnerabilities across cloud layers, compromising cryptographic foundations and critical services.

We identify quantum-exploitable vulnerabilities across cloud components: classical encryption susceptibility requiring PQC adoption with key management, efficiency, and interoperability challenges; side-channel risks in multi-tenant Virtual Machines (VMs)/containers; PQC computational overhead impacting scalability; security gaps during hybrid transition; and evolving quantum-safe regulatory requirements. Addressing these vulnerabilities is critical for quantum-resistant cloud security.

Quantum Attack Vectors for Quantum-Safe Cryptography. Quantum adversaries may exploit SCAs vulnerabilities in PQC implementations, compromising NIST-standardized algorithms despite their mathematical quantum resistance. We assess risks for each attack vector documented in Table VII through comprehensive qualitative risk assessment integrating likelihood evaluation and impact analysis (Figure 4). 3.2.4 Likelihood and Impact Evaluation. Likelihood assessment examines three factors: exploitability characteristics (physical/network/internet access requirements),

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410034

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

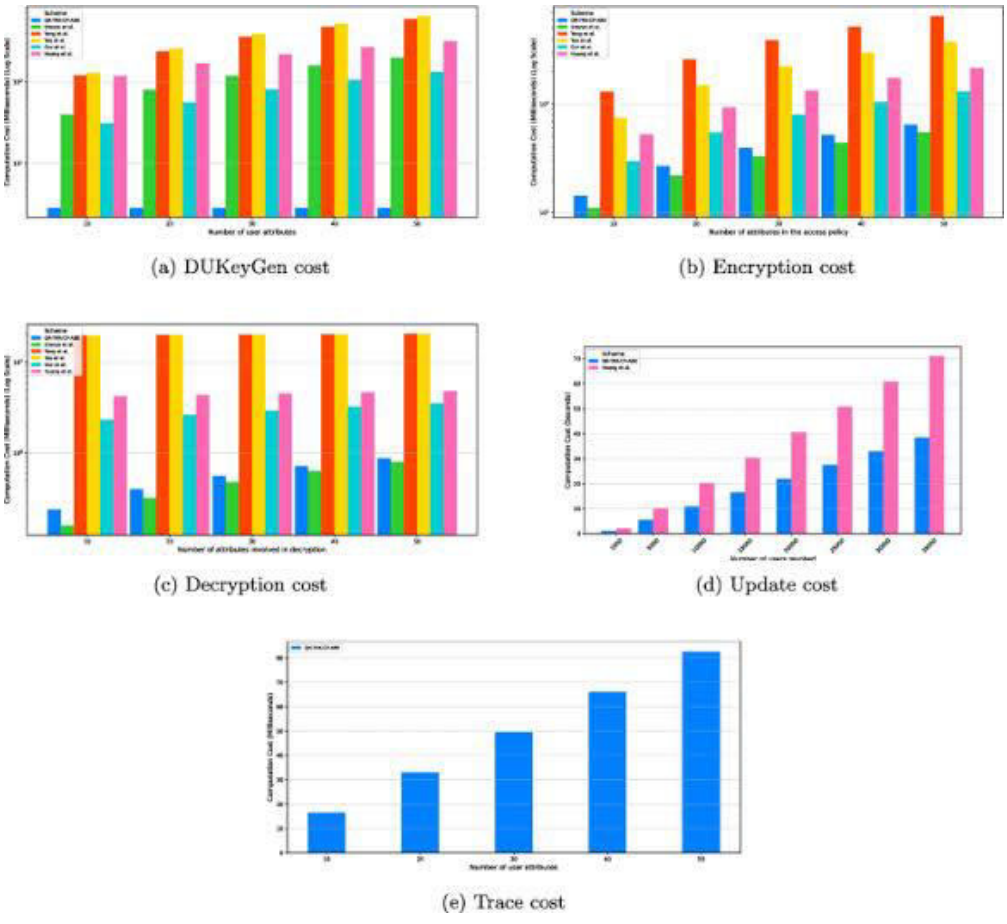
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

countermeasure availability and effectiveness (detailed in Table VII), and NIST SP 800-30 Appendix G criteria [21] adapted for quantum threat scenarios (Table IV). We categorize likelihood as: (a) High - known remote exploit with no effective countermeasures; (b) Medium - known exploit requiring physical access without adequate countermeasures; (c) Low - no known exploit, or exploit mitigated by effective countermeasures, or attack requires elevated privileges. Impact assessment applies NIST SP 800-30 Appendix H criteria [21] with quantumspecific adaptations (Table V). Quantum-enabled threats can compromise data confidentiality and integrity, disrupt service availability, damage organizational reputation, or trigger regulatory violations. Given these potential consequences, quantum threats warrant minimum medium baseline impact.

IV. RESULT ANALYSIS

To understand the risks posed by QC, we analyze quantum computer emergence timelines spanning 5 to 30 years, based on cumulative expert likelihood assessments [36]. Figure 5 summarizes expert opinions on when quantum computers capable of breaking classical cryptography will emerge. We define quantum threat as the probability that a quantum computer can break RSA-2048 encryption within 24 hours. These probability assessments can be extended to evaluate the likelihood of breaking other cryptographic algorithms based on their quantum security levels.

Risk is assessed by combining likelihood and impact using a qualitative matrix (Figure 4) mapping combinations to risk levels. High-risk scenarios demand immediate mitigation; medium-risk scenarios require planned responses; low-risk scenarios may be monitored or accepted based on risk tolerance. This systematic assessment prioritizes quantum risks, enabling informed quantum-safe transition decisions.



(a) DUKeyGen cost (b) Encryption cost

(c) Decryption cost (d) Update cost

(e) Trace cost

Fig 2: Quantum-resistant traceable, revocable

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CC infrastructures are structured across nine architectural layers (applications, data, runtime, middleware, OS, virtualization, server, storage, and networks) as illustrated in Figure 1. This section assesses the quantum threat landscape during the pre-transition phase, when cloud environments still rely on vulnerable classical cryptographic standards. Building on vulnerabilities discussed in Section III, we systematically analyze how quantum-enabled adversaries exploit each layer's cryptographic and architectural dependencies, exposing systemic risks. Delayed deployment of quantum-resistant primitives further amplifies exposure to attacks such as key recovery, ciphertext harvesting for future decryption, and signature forgeries. To guide early-stage defense planning, we emphasize the need for tailored threat modeling and layered mitigation strategies aligned with each architectural layer.

V. CONCLUSION

Enabling layer-specific mitigation strategies for communication protocols, PKI, KMS, and control planes. Our analysis shows that hybrid cryptographic deployments are essential for mitigating HNDL risks while preserving backward compatibility during migration. A technical evaluation of NIST-standardized PQC algorithms revealed significant implementation, performance, and deployment challenges, notably susceptibility to SCA and fault attacks in multi-tenant environments involving shared VMs, accelerators, and TEEs. Furthermore, a comparative study of AWS, Azure, and GCP highlighted progress in cryptographic agility and HSM integration, while exposing persistent gaps in interoperability and deployment maturity. Overall, securing the quantum-era cloud requires coordinated evolution across cryptographic infrastructure, governance, and workforce preparedness. Future research should prioritize standardization, hardware-based performance optimization, AI-enhanced threat mitigation, and automated, policy-driven, crypto-agile migration frameworks to sustain long-term resilience and trust in global cloud ecosystems.

REFERENCES

[1] Amit Sahai, and Brent Waters, "Fuzzy Identity-Based Encryption," *Advances in Cryptology – EUROCRYPT*, vol. 3494, pp. 457-473, 2005.
[CrossRef] [Google Scholar] [Publisher Link]
[2] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.
[CrossRef] [Google Scholar] [Publisher Link]
[3] Junbeom Hur, and Dong Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2011.
[CrossRef] [Google Scholar] [Publisher Link]
[4] Vipul Goyal et al., "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89-98, 2006.
[CrossRef] [Google Scholar] [Publisher Link]
[5] Melissa Chase, "Multi-Authority Attribute Based Encryption," *Theory of Cryptography*, vol. 4392, pp. 515-534, 2007.
[CrossRef] [Google Scholar] [Publisher Link]
[6] Van-Hoan Hoang, Elyes Lehtihet, and Yacine Ghamri-Doudane, "Forward-Secure Data Outsourcing Based on Revocable Attribute-Based Encryption," *15th International Wireless Communications & Mobile Computing Conference*, pp. 1839-1846, 2019.
[CrossRef] [Google Scholar] [Publisher Link]
[7] Hongjian Yin et al., "A Traceable CP-ABE Scheme Supporting Dynamic Revocation and Efficient Decryption for Medical Data Sharing," *IEEE Internet of Things Journal*, vol. 12, no. 24, pp. 53610-53622, 2025.
[CrossRef] [Google Scholar] [Publisher Link]
[8] Shuaishuai Chang et al., "T-ABE: A Practical ABE Scheme to Provide Trustworthy Key Hosting on Untrustworthy Cloud," *IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 960-967, 2024.
[CrossRef] [Google Scholar] [Publisher Link]
[9] Sravya Gudipati, Syam Kumar Pasupuleti, and R. Padmavathy, "Quantum-Resistant Traceable, Revocable, and Key Escrow-Free CP-ABE for Cloud Storage," *Peer-to-Peer Networking and Applications*, vol. 18, 2025.
[CrossRef] [Google Scholar] [Publisher Link]
[10] Alejandro Peñuelas-Angul, Claudia Feregrino-Uribe, and Miguel Morales-Sandoval, "A Revocable Multi-Authority Attribute-Based Encryption Scheme for Fog-Enabled IoT," *Journal of Systems Architecture*, vol. 155, 2024.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[CrossRef] [Google Scholar] [Publisher Link]
[11] L.F. Guo, X.M. Xing, and H. Guo, "An Efficient Traceable and Revocable Attribute-Based Encryption Scheme for Cloud Storage," Journal of Cryptology, vol. 10, no. 1, pp. 131-145, 2023.
[Google Scholar]
[12] Kai Zhang et al., "A Traceable and Revocable Multiauthority Attribute-Based Encryption Scheme with Fast Access," *Security and Communication Networks*, vol. 2020, pp. 1-14, 2020.
[CrossRef] [Google Scholar] [Publisher Link]
[13] Melissa Chase, and Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pp. 121-130, 2009.
[CrossRef] [Google Scholar] [Publisher Link]
[14] Huang Lin et al., "Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority," *Information Sciences*, vol. 180, no. 13, pp. 2618-2632, 2010.
[CrossRef] [Google Scholar] [Publisher Link]
[15] Y. Liu, S. Xu, and Z. Yue, "Partially Hidden Policy Multi-Authority CP-ABE Scheme with Constant Length Ciphertext", Journal on Communications, vol. 45, no. 8, pp. 20-36, 2024.
[CrossRef] [Google Scholar] [Publisher Link]
[16] Guangli Xiang et al., "An Attribute Revocable CP-ABE Scheme," *Seventh International Conference on Advanced Cloud and Big Data*, pp. 198-203, 2019.
[CrossRef] [Google Scholar] [Publisher Link]



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details