Frontiers in Emerging Engineering & Technologies (Open Access)

Volume 03, Issue 01, January 2026,
DOI: - https://doi.org/10.64917/feet/Volume03Issue01-01 PageNo.01-12

Post-Quantum Cryptography in Identity and Access Management: Readiness, Transition Strategies, and Compliance Implications

Pulipati, Kiran Kumar
Department of Information Studies, Trine university, USA

RECEIVED - 11-20-2025, **RECEIVED REVISED VERSION** - 12-27-2025, **ACCEPTED**- 12-31-2025, **PUBLISHED**- 01-02-2026

Abstract

The swift rise in quantum computing casts a shadow on the efficacy of traditional IAM sheds. This research paper intends to define the 'readiness 'state of the IAM framework in relation to post-quantum cryptography (PQC) and the methodological approach needed to protect the transition. This focuses on the authentication, encryption and digital signing in the RSA, ECC, and Diffie-Hellman whos ease of access has been compromised to quantum computing. The case studies assess complexities such as RSA, ECC, and the Diffie-Hellman algorithm for authentication and encryption, alongside NIST policies, to configure the architecture. This also studies the policies on paramount underlying NIST HIPAA and GDPR that argue for slow, stepped migration to IM in the IAM framework. The research still retains quantum attacks as the foremost assaults to enterprise blockchain. As the case studies suggest, immense risks are associated with the rapidly emerging fundamental notions of interactivity, practicality, and IAM cryptography. Thus, the NIST PQC strategy possession and digital signing restraints suggest implementing a pluralistic encryption model and advocating compliance with the quartet that lowers the threshold to cryptography protected by PQC. The NIST HIPAA policies assert certain presumptions, as formulated, are presumed rational with more than sufficient backbone, and remain warm, unfrozen. The outcome is confident in saying that IAM frameworks require foresight while algorithmically synthesising responses to counter aggressor base… quantum-related forces.

Keywords: Post-quantum cryptography, IAM security, PQC transition, NIST standards, RSA vulnerability, ECC threat, hybrid cryptography, key management, compliance, quantum resilience

1.Introduction

The rapid evolution of quantum computing challenges traditional "IAM security" mechanisms. Classical algorithms like "RSA" and "ECC" are vulnerable to quantum attacks, risking sensitive data. "Post-quantum cryptography" aims to replace these algorithms with quantum-resistant alternatives. Implementing "PQC transition" requires hybrid approaches combining classical and quantum-safe cryptography. NIST standards guide secure migration, ensuring "compliance" with HIPAA and GDPR frameworks. "Digital signing" mechanisms also need upgrading for quantum resilience. Effective "key management" is essential to maintain cryptographic integrity during transition. IAM frameworks must integrate pluralistic encryption strategies to resist quantum adversaries. Case studies highlight practical implementation challenges in authentication, encryption, and access control. This research evaluates "quantum resilience" while addressing risks from interactivity and performance in enterprise systems. This study further explores organizational preparedness, governance alignment, and interoperability of quantum-safe solutions. It emphasizes continuous monitoring, employee training, and adaptive cryptographic agility to sustain long-term IAM security resilience.

1.1 Research objectives:

- To assess IAM frameworks' readiness for post-quantum cryptography in authentication and

encryption.

- To analyze transition strategies for migrating RSA, ECC, and Diffie-Hellman to PQC.
- To examine compliance implications under NIST, HIPAA, and GDPR for PQC adoption.
- To evaluate quantum threats on blockchain and propose a resilient pluralistic encryption model.

1.2 Research Questions:

• How ready are IAM frameworks for post-quantum cryptography in authentication and encryption?
• What transition strategies support migrating RSA, ECC, and Diffie-Hellman to PQC?
• How do NIST, HIPAA, and GDPR compliance requirements impact PQC adoption?
• How can blockchain withstand quantum threats through a resilient pluralistic encryption model?

2. Literature

Post-quantum cryptography (PQC) is crucial for securing identity and access management (IAM) systems against upcoming quantum threats (Mamatha *et al.,* 2024). Traditional algorithms like "RSA," "ECC," and "Diffie-Hellman" are increasingly at risk to quantum attacks, threatening sensitive authentication and encryption processes. Researchers emphasize adopting "PQC transition" approaching that integrate hybrid cryptographic models, integrating classical and quantum-resistant algorithms to ensure smooth migration without disrupting existing IAM activities. NIST has finalised standards, including CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for "digital signing," providing clear guidance for implementing quantum-safe frameworks (Ricci *et al*., 2021). Compliance with regulations such as HIPAA and GDPR also drives organisations to adopt PQC, as regulatory bodies highlight the importance of maintaining data protection even under quantum threats. Experts argue that "key management" becomes more critical in this transition, as secure storage and rotation of cryptographic keys ensure data integrity (Guthoff *et al.,* 2023). Implementing PQC also requires testing for performance overhead, as some quantum-safe algorithms may introduce computational delays affecting IAM efficiency. Scholars note that hybrid cryptography permits enterprises to sustain authentication, encryption, and access control while progressively integrating quantum-resistant processes. Literature underscores that IAM frameworks need foresight, planning, and continuous supervising to resist quantum adversaries successfully (Cultice *et al.,* 2023). Case studies highlight real-world complexities in upgrading authentication protocols, digital signing, and encryption processes while complying with both technical standards and legal requirements. Therefore, experts agree that proactive adoption of PQC, guided by NIST standards and regulatory compliance, enhances "quantum resilience" in IAM systems, secures sensitive information, and provides a sustainable framework for future-proof enterprise security against quantum-enabled attacks.

Previous researchers in 2020, such as Chen et al. (2020), focused mainly on quantum-safe algorithm design. This study extends their work by exploring IAM readiness, compliance alignment, and practical PQC transition strategies in enterprise environments.

3. Method

This study employed a secondary research method to analyse "post-quantum cryptography." Peer-reviewed journals, technical reports, and case studies provided detailed insights into IAM frameworks. Using secondary data allowed the evaluation of existing "RSA," "ECC," and "Diffie-Hellman" vulnerabilities efficiently. NIST guidelines and regulatory documents were reviewed to assess compliance under "HIPAA" and "GDPR" (Ettaloui *et al.*, 2023).

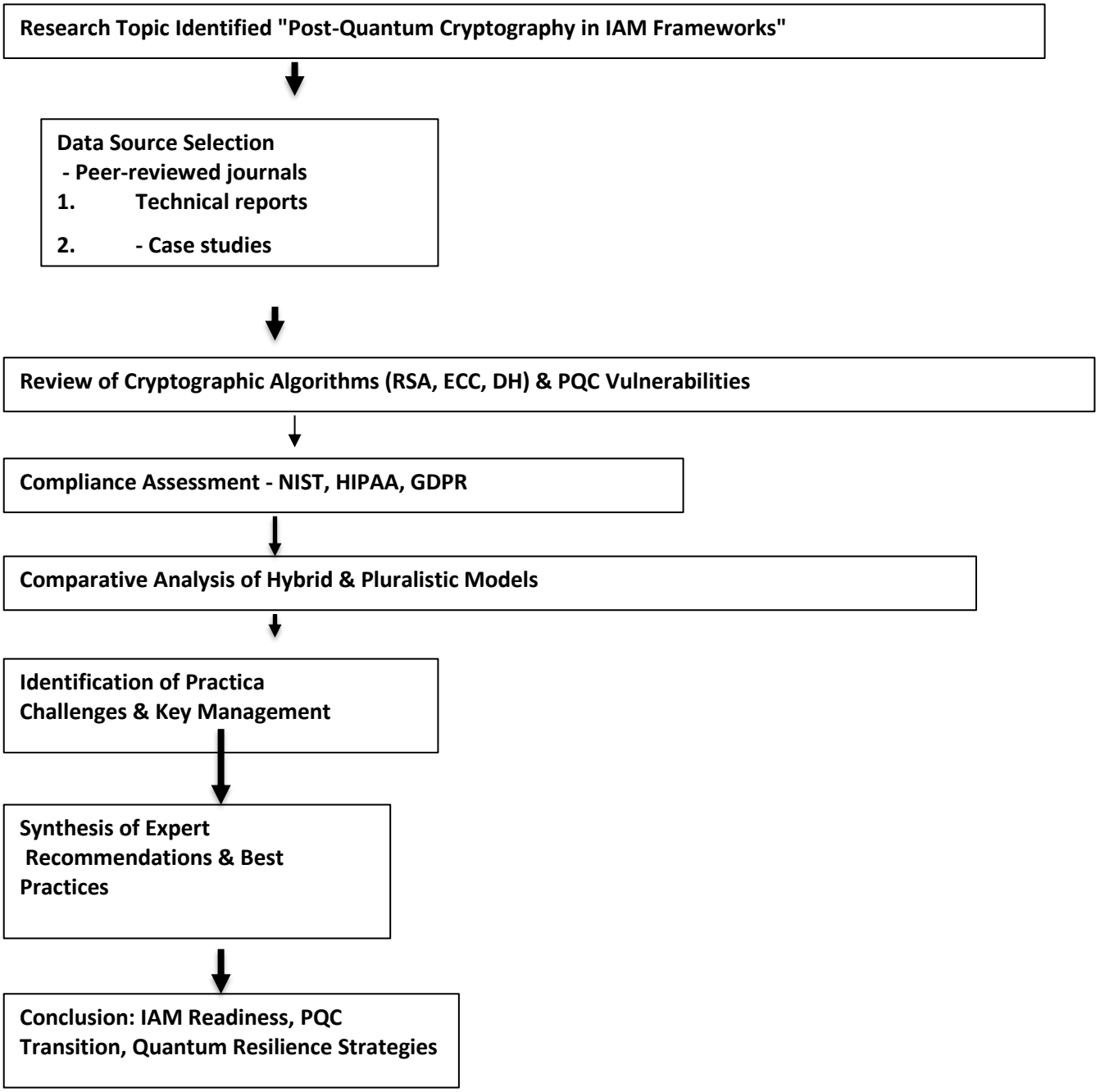

Figure 1: Secondary Research on Post-Quantum Cryptography in IAM

Secondary research enabled comparison of hybrid and pluralistic encryption models across multiple organisations. Historical implementation data helped identify practical challenges in "PQC transition." It reduced time and cost compared to primary experimentation or simulations. Existing studies provided evidence on computational overhead and "key management" complexities during migration. The method allowed the synthesis of expert recommendations and best practices for IAM security (Anderson *et al.*, 2022). Secondary sources offered quantitative metrics and qualitative analysis for "digital signing" and authentication improvements. Overall, this approach ensured comprehensive coverage of "quantum resilience" strategies while maintaining reliability, efficiency, and technical depth. Using secondary data strengthened the research's validity and supported actionable conclusions for enterprise IAM adoption.

4. Results

4.1 Readiness of IAM for Post-Quantum Cryptography

The readiness of IAM for "post-quantum cryptography" remains limited in current systems. Traditional "RSA" and "ECC" keys are vulnerable to Shor's quantum algorithm attacks (Sharath *et al.,* 2025). Most IAM frameworks still rely on classical encryption for authentication and digital

signing. Studies show hybrid models combining classical and "PQC transition" algorithms enhance gradual adoption. Key management practices require upgrading to handle larger PQC keys efficiently. NIST recommends using CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for signatures (Ricci *et al*.,2021).

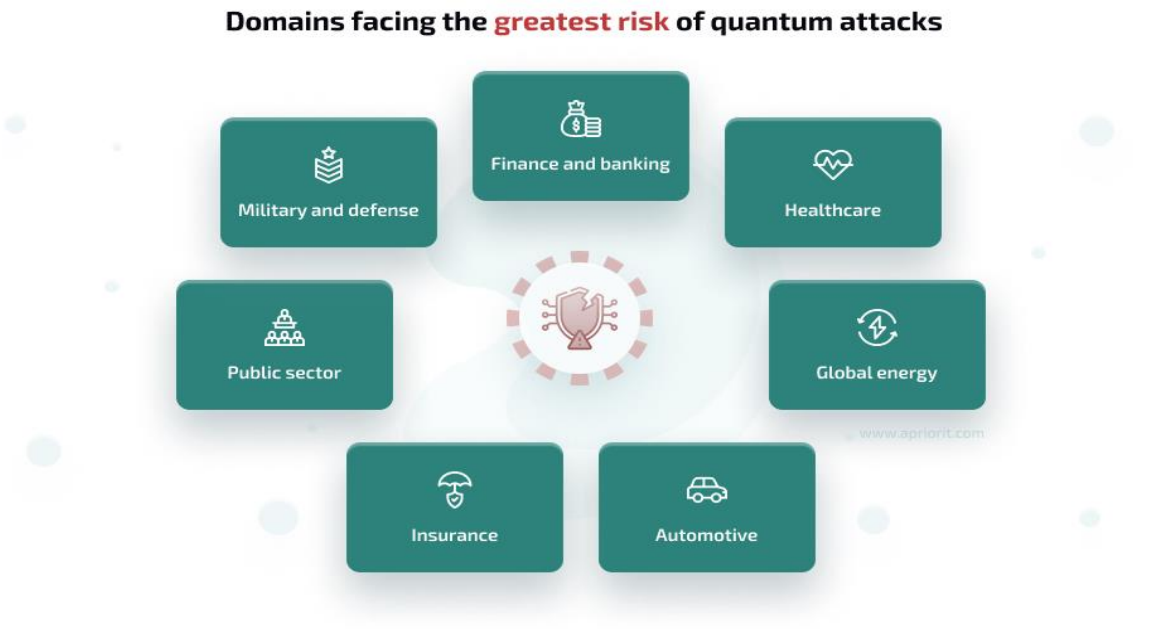

Figure 2: Domains facing the greatest risk of quantum attacks

(Source: Apriorit, 2022)

Many enterprise IAM systems lack integration with lattice-based or hash-based cryptography modules. Access control mechanisms must adapt to support quantum-safe token exchanges and certificate verification. Multi-factor authentication schemes need quantum-resistant underlying cryptographic primitives. Legacy Single Sign-On (SSO) protocols face interoperability issues with PQC algorithms. Testing indicates that PQC introduces higher computational overhead and latency in authentication flows. IAM readiness also depends on compliance with GDPR and HIPAA during migration. Automated key rotation and lifecycle management are critical for maintaining PQC integrity (Aramide *et al*., 2022). Security monitoring tools must detect quantum-specific threat patterns. Case studies highlight difficulties in scaling PQC across distributed IAM architectures. Organisations with proactive cryptographic audits show faster PQC adaptation. Overall, current IAM frameworks require structured migration plans, hybrid encryption models, and compliance-aligned "quantum resilience" strategies. The technical gap between existing IAM and PQC mandates immediate strategic upgrades.

4.2 Vulnerabilities of Classical Algorithms (RSA, ECC, Diffie-Hellman)

Classical algorithms like "RSA," "ECC," and "Diffie-Hellman" are highly vulnerable to quantum attacks. Shor's algorithm can efficiently factor large "RSA" keys, breaking encryption rapidly. Similarly, "ECC" discrete logarithms are compromised under quantum computation, exposing private keys (Tom *et al*., 2023). "Diffie-Hellman" key exchanges are susceptible to quantum adversaries, risking session confidentiality. Studies show key lengths once considered secure are now insufficient against quantum capabilities. Large prime generation in "RSA" becomes irrelevant under quantum factorisation methods. "ECC" curves lose cryptographic strength, making digital signing insecure. Many IAM frameworks still depend on these classical primitives for authentication.

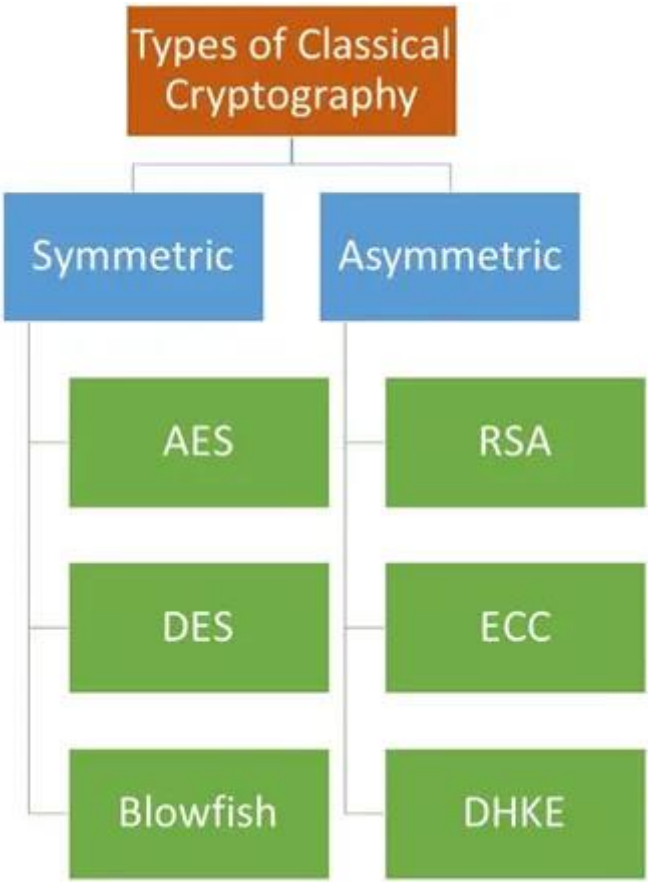

Figure 3: State-of-the-art analysis of quantum cryptography

(Source: Swastik Kumar et al., 2024)

Hybrid solutions combining "PQC transition" algorithms are recommended to mitigate quantum threats. Research indicates that lattice-based and hash-based schemes provide higher quantum resilience. Quantum attacks reduce computational security from exponential to polynomial time complexity. Legacy protocols relying on classical algorithms face interoperability challenges during PQC migration. "Digital signing" mechanisms built on classical algorithms risk forgery in quantum scenarios (Vakarjuk *et al.*, 2024). Cryptanalysis studies highlight vulnerability in ephemeral key exchanges over untrusted channels. NIST guidance recommends immediate assessment of "RSA" and "ECC" usage in IAM systems. Organisations are advised to inventory cryptographic assets and prepare phased upgrades. Classical random number generators and entropy sources may require enhancement for PQC readiness. Overall, the inherent weaknesses of "RSA," "ECC," and "Diffie-Hellman" emphasise urgent adoption of quantum-safe alternatives (Aldarwbi *et al.,* 2024). IAM frameworks must integrate hybrid cryptography and robust "key management" to ensure secure authentication.

4.3 Transition Complexities and NIST-Guided Strategies

Transitioning IAM frameworks to "post-quantum cryptography" involves significant technical complexities. Hybrid cryptography models are necessary to maintain compatibility with legacy "RSA" and "ECC" systems. Key size increases in lattice-based algorithms impact performance and storage requirements. NIST-guided strategies emphasise phased migration and "PQC transition" planning.

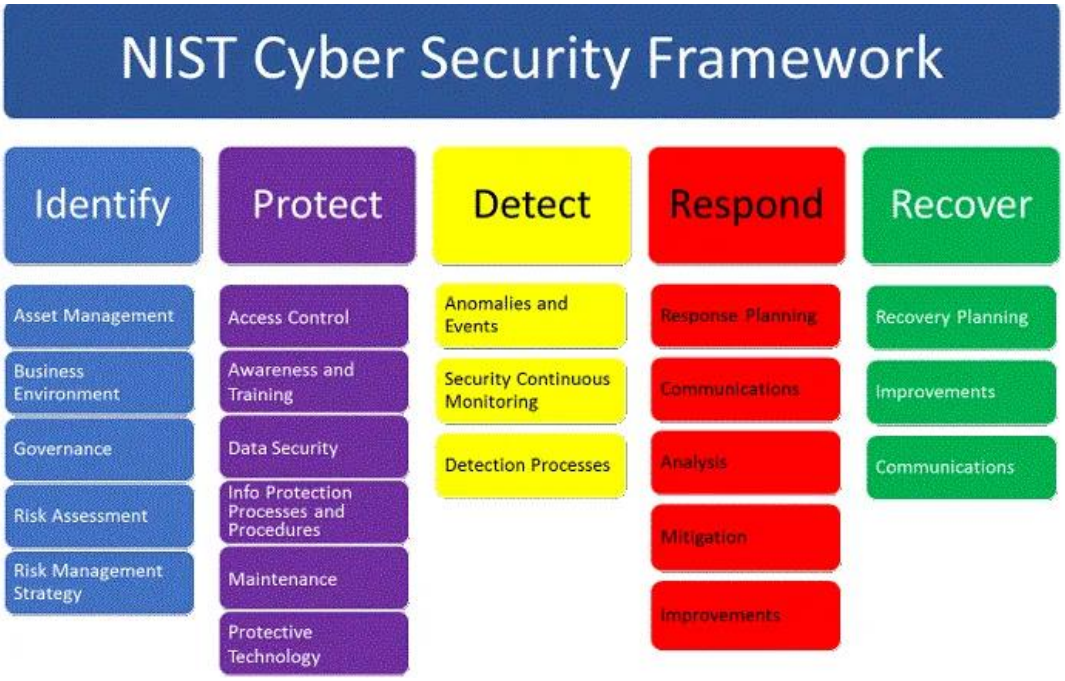

Figure 4: NIST cybersecurity framework

Source: Darkreading, 2020

Organisations must audit existing cryptographic assets for algorithm vulnerabilities. "Digital signing" processes require updating to quantum-resistant schemes like CRYSTALS-Dilithium. Session key exchanges must adopt lattice-based or hash-based encryption for quantum safety. Multi-factor authentication protocols need quantum-secure underlying primitives for token verification. NIST recommends rigorous testing of hybrid implementations to ensure functional interoperability (Olorunlana *et al.,* 2024). Key management frameworks must handle increased key lengths and rotation frequency efficiently. Compliance with HIPAA and GDPR must be guaranteed throughout the transition. Legacy SSO and associated personhood systems face unification challenges with quantum-resistant methods. Case studies show migration overhead can impact authentication latency and user experience. Automated monitoring tools are essential to detect misconfigurations during PQC adoption. Organisations must implement rollback mechanisms in case of transition failures. Education and training of IAM administrators on "quantum resilience" best practices is critical. NIST standards provide a roadmap for secure, compliant, and gradual deployment (Paul *et a*l., 2023). Overall, IAM systems require careful planning, hybrid cryptography, and rigorous "key management" for quantum readiness (Singh *et al*., 2023). The transition emphasises balancing performance, security, and compliance across enterprise identity infrastructures.

4.4 Compliance Implications under HIPAA and GDPR

Compliance with "HIPAA" and "GDPR" poses critical challenges for post-quantum IAM. These regulations require protection of sensitive health and personal data at all times (Jurczuk *et al*., 2024). Classical algorithms like "RSA" and "ECC" no longer provide sufficient quantum resilience. Organisations must adopt "PQC transition" strategies to maintain regulatory adherence. NIST-guided standards help ensure "digital signing" and encryption meet legal requirements. Data breach risks increase if legacy cryptography remains unmodified under quantum threats. IAM systems must implement "key management" policies supporting larger PQC keys (Singh *et al*., 2023). Multi-factor authentication and SSO protocols require updates for quantum-secure operations. Regulatory audits demand proof of compliance and evidence of secure cryptographic migration. Encryption and authentication mechanisms must be documented and tested rigorously.

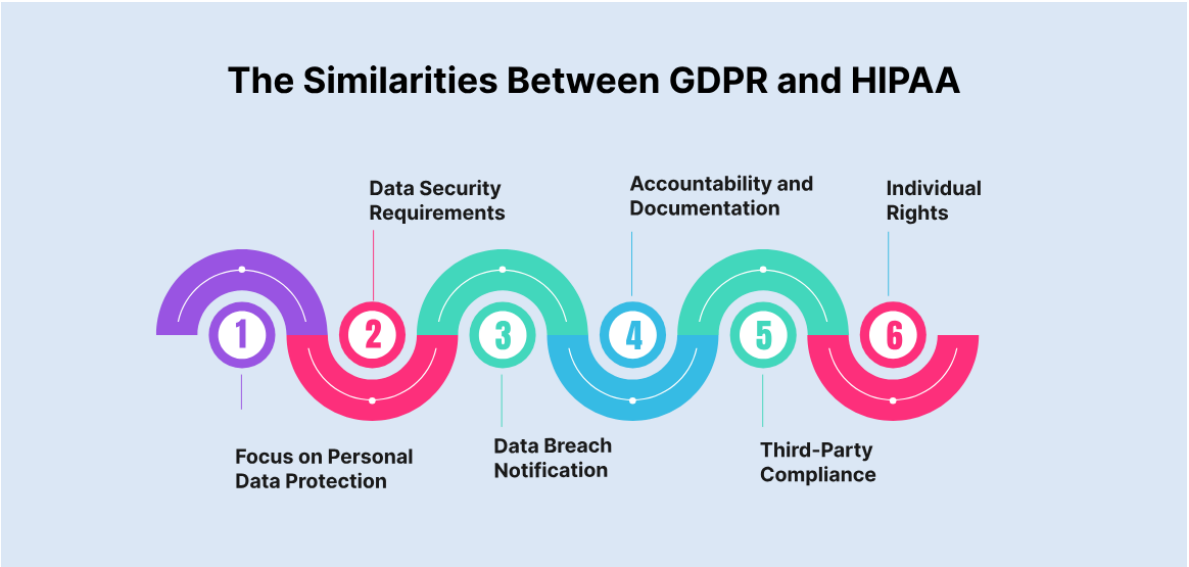

Figure 5: The similarities between GDPR and HIPAA

(Source: Sunil Kumar, 2025)

Automated monitoring ensures sensitive data access aligns with HIPAA and GDPR. Data retention, processing, and transfer practices require PQC-compatible protocols. Organisations must map cryptographic assets to regulatory obligations to reduce legal exposure. Failure to adopt quantum-resistant measures can result in penalties and reputational loss. Case studies show enterprises with proactive PQC adoption demonstrate a stronger compliance posture. Overall, integrating "quantum resilience" into IAM ensures secure authentication, encryption, and regulatory adherence (UZOKA *et al.*, 2021). Continuous evaluation and reporting are essential to maintain compliance under evolving quantum threats. Compliance strategies must align technical upgrades with legal obligations effectively and efficiently.

4.5 Adoption of Hybrid and Pluralistic Encryption Models

Adopting "hybrid cryptography" and "pluralistic encryption" models strengthens IAM against quantum threats. Hybrid approaches combine classical algorithms like "RSA" and "ECC" with "post-quantum cryptography" primitives. This ensures continuity during "PQC transition" without disrupting existing authentication and encryption workflows. Pluralistic encryption uses multiple quantum-safe algorithms simultaneously, increasing resistance against unforeseen quantum attacks (Vyavahare, 2025). Key management frameworks must handle diverse key types, sizes, and lifecycles efficiently. Digital signing processes require integration of lattice-based or hash-based signatures alongside classical schemes. Multi-factor authentication protocols benefit from hybrid encryption to secure token exchanges.

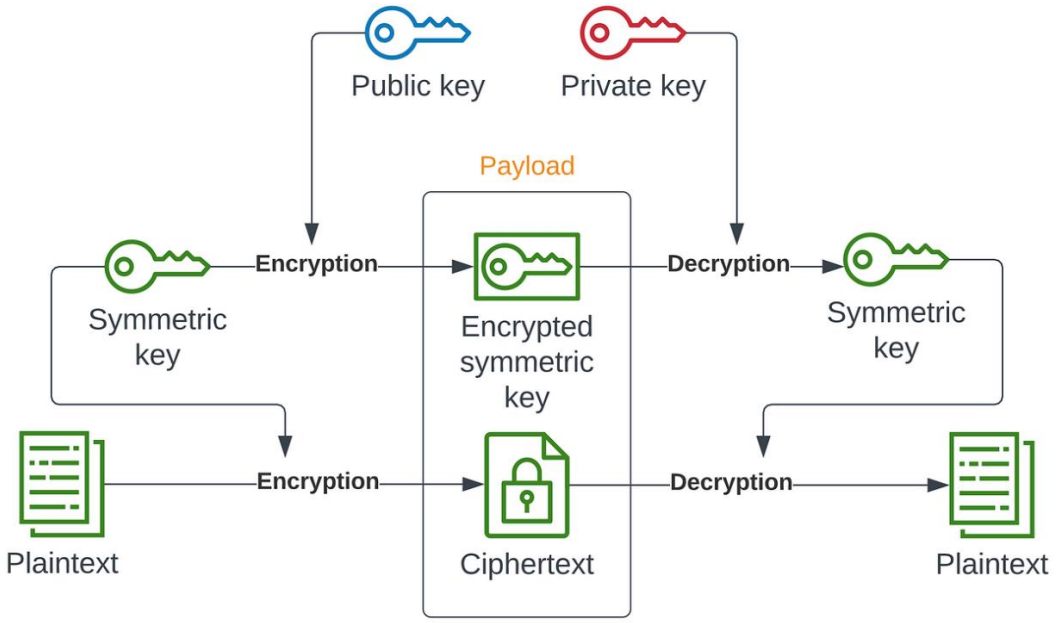

Figure 6: Hybrid Cryptography

(Source: Umesh Kumar, 2024)

Hybrid models reduce migration risk by allowing phased replacement of vulnerable algorithms. Studies demonstrate computational administrative costs growth but remains manageable with optimized cryptographic libraries. NIST-guided standards support hybrid deployment, ensuring compatibility and adherence with HIPAA and GDPR (Zhou *et al.,* 2024). Automated monitoring tools detect misconfigurations or weak algorithm combinations in hybrid setups. Organisations with hybrid strategies demonstrate improved "quantum resilience" without fully decommissioning legacy systems. Pluralistic encryption further mitigates single-point cryptographic failures across distributed IAM architectures. Case studies show enhanced protection in authentication, data encryption, and digital signing. Overall, hybrid and pluralistic models provide practical, compliant, and secure pathways for quantum-safe IAM adoption. These approaches balance performance, security, and regulatory adherence during the complex PQC migration process (Wiesmaier *et al.,* 2021). Effective implementation requires planning, auditing, and rigorous "key management" across all IAM components.

5. Discussion

The findings highlight critical gaps in IAM's readiness for "post-quantum cryptography." Classical algorithms like "RSA," "ECC," and "Diffie-Hellman" are inherently vulnerable to Shor's algorithm attacks (SS *et al*., 2024). This exposes authentication, encryption, and "digital signing" processes to quantum adversaries. Transitioning requires "PQC transition" strategies that integrate hybrid and pluralistic encryption models. Hybrid cryptography guarantees consistency with legacy systems while presenting quantum-resistant primitives. Pluralistic cryptography enhances security by integrating multiple algorithms concurrently, minimizing single-point malfunctions. However, these approaches increase computational overhead, affecting authentication latency and key lifecycle management.

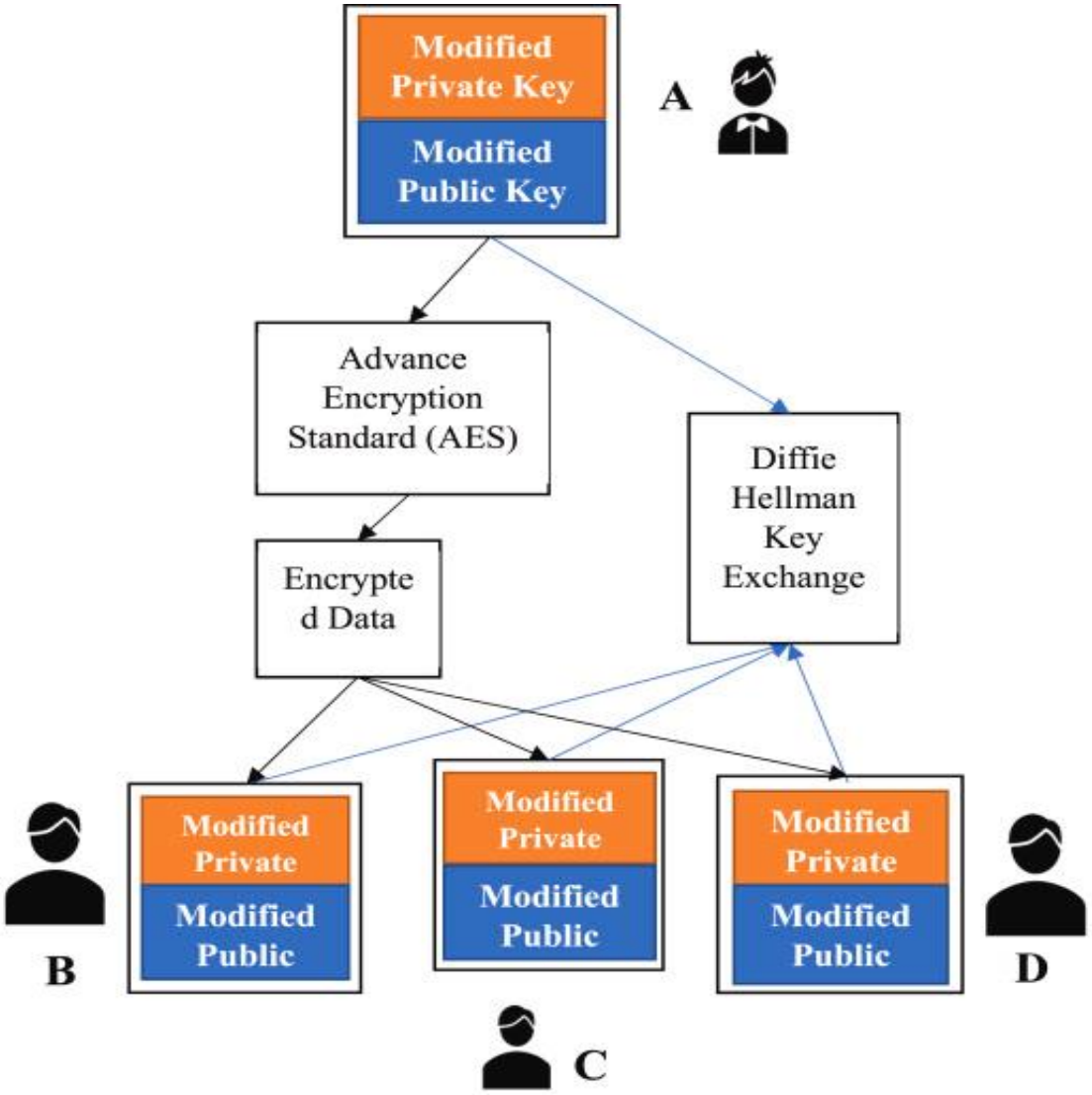

Figure 7: A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security

(Source: B. Ranganatha Rao *et al*., 2023)

"Key management" frameworks must handle larger, complex PQC keys efficiently to maintain security integrity (Marchsreiter *et al.,* 2025). NIST standards provide structured migration roadmaps but require careful implementation to avoid interoperability issues. Compliance with "HIPAA" and "GDPR" adds additional complexity, as encryption and signing processes must meet strict regulatory standards. Automated supervising and auditing become essential to detect incorrect settings or weak cryptographic blends. Legacy SSO, allied identity, and multi-factor validation protocols must be upgraded with quantum-secure primitives. Case studies reveal phased relocation minimizes operational interruption but demands extensive preparation, testing, and training. Overall, the findings underscore that IAM frameworks cannot rely solely on classical algorithms (Mohan *et al.,* 2025). Organisations must adopt hybrid and pluralistic strategies, enforce rigorous "key management," and ensure compliance. The combination of technical upgrades and regulatory adherence is crucial to achieving effective "quantum resilience" in enterprise IAM systems.

6. Conclusion

This research confirms IAM frameworks are unprepared for "post-quantum cryptography." Classical algorithms like "RSA," "ECC," and "Diffie-Hellman" are vulnerable to quantum attacks. Hybrid and pluralistic encryption models provide practical solutions for "PQC transition." NIST standards guide secure migration while ensuring compliance with "HIPAA" and "GDPR." Effective "key management" is essential for handling larger quantum-safe keys. IAM systems require updates in authentication, encryption, and "digital signing" mechanisms. Phased migration reduces operational disruption and enhances

"quantum resilience" across enterprise infrastructures. Automated monitoring and auditing ensure regulatory adherence and detect misconfigurations. Case studies show technical complexities in scaling hybrid solutions remain significant. Overall, proactive implementation of quantum-resistant strategies strengthens IAM security, preserves regulatory observance.

Future Research Directions:

Future studies should explore real-world PQC deployment in large-scale IAM systems. Integrating AI-driven key management and blockchain-based authentication can further enhance adaptive quantum resilience and automation.

Limitations:

This research relied on secondary data, limiting experimental validation. Lack of real-time PQC testing and restricted enterprise datasets may affect the accuracy of assessing IAM transition readiness and performance.

References

1. Aldarwbi, M., Ghorbani, A.A. and Lashkari, A.H., 2024. The Quantum Shift in Group Communication: A Review and Analysis of Group Key Establishment from Classical to Advanced Quantum-Safe and Quantum-Based Solutions. Authorea Preprints. Available at https://www.techrxiv.org/doi/full/10.36227/techrxiv.173221587.74899261
2. Anderson, J. and Nguyen, A., 2022. The Role of Identity and Access Management (IAM) in Securing Cloud Workloads. ResearchGate December. Available at https://www.researchgate.net/profile/Jessie-Anderson-8/publication/389518277_The_Role_of_Identity_and_Access_Management_IAM_in_Securing_Cloud_Workloads/links/67c660108311ce680c7b90d9/The-Role-of-Identity-and-Access-Management-IAM-in-Securing-Cloud-Workloads.pdf
3. Aramide, O.O., 2022. Post-Quantum Cryptography (PQC) for Identity Management. ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES, 12(02), pp.59-67. Available at https://smsjournals.com/index.php/Adhyayan/article/view/3373
4. Available at https://dl.acm.org/doi/abs/10.1145/3465481.3465756
5. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2020). *Report on Post-Quantum Cryptography.* NISTIR 8105. National Institute of Standards and Technology.
6. Cultice, B., Irwin, E. and Jones, M., 2023. Accounting for spatial economic interactions at local and meso scales in integrated assessment model (IAM) frameworks: challenges and recent progress. Environmental Research Letters, 18(3), p.035009. Available at https://iopscience.iop.org/article/10.1088/1748-9326/acbce6/meta
7. Ettaloui, N., Arezki, S. and Gadi, T., 2023. An overview of blockchain-based electronic health records and compliance with GDPR and HIPAA. Data and Metadata, 2, pp.166-166. Available at https://scholar.archive.org/work/cuf2bptrjbdfdbosywp4obcq2q/access/wayback/https://dm.saludcyt.ar/index.php/dm/article/download/166/307
8. Guthoff, C., Anell, S., Hainzinger, J., Dabrowski, A. and Krombholz, K., 2023, May. Perceptions of distributed ledger technology key management-an interview study with finance professionals. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 588-605). IEEE. Available at https://ieeexplore.ieee.org/abstract/document/10335652/
9. Jurczuk, M. and Suprunowicz, M., 2024. Consent in data privacy: a general comparison of GDPR and HIPAA. Przegląd Prawniczy Uniwersytetu im. Adam Mickiewicza, 16, pp.173-194. Available at https://www.ceeol.com/search/article-detail?id=1343065
10. Mamatha, G.S., Dimri, N. and Sinha, R., 2024. Post-quantum cryptography: Securing digital communication in the quantum era. arXiv preprint arXiv:2403.11741. Available at https://smsjournals.com/index.php/Adhyayan/article/view/3373
11. Marchsreiter, D., 2025. Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems. IET Blockchain, 5(1), p.e12094. Available at https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/blc2.12094

12. Mohan, D.R., 2025. AI-Driven Integration of Legacy IAM Services into AWS Cloud-Based Microservice Architectures: A Scalable Framework for Secure Identity Management. Available at https://philpapers.org/rec/RAJAIO

13. Olorunlana, T.J., 2024. Securing Healthcare Data in the Cloud under HIPAA and NIST Frameworks [online] Available at https://www.researchgate.net/profile/Taiwo-Olorunlana/publication/393609684_Securing_Healthcare_Data_in_the_Cloud_under_HIPAA_and_NIST_Frameworks/links/68713c44dd6b84447df7e4c0/Securing-Healthcare-Data-in-the-Cloud-under-HIPAA-and-NIST-Frameworks.pdf

14. Paul, J., 2023. Regulatory Compliance and Zero Trust: How Organizations Can Meet NIST 800-207, GDPR, and HIPAA Standards. Available at https://www.researchgate.net/profile/Joel-Paul-10/publication/389166942_Regulatory_Compliance_and_Zero_Trust_How_Organizations_Can_Meet_NIST_800-_207_GDPR_and_HIPAA_Standards/links/67b7306cf5cb8f70d5b5de65/Regulatory-Compliance-and-Zero-Trust-How-Organizations-Can-Meet-NIST-800-207-GDPR-and-HIPAA-Standards.pdf

15. Ricci, S., Malina, L., Jedlicka, P., Smékal, D., Hajny, J., Cibik, P., Dzurenda, P. and Dobias, P., 2021, August. Implementing CRYSTALS-Dilithium signature scheme on FPGAs. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-11). Available at https://dl.acm.org/doi/abs/10.1145/3465481.3465756

16. Ricci, S., Malina, L., Jedlicka, P., Smékal, D., Hajny, J., Cibik, P., Dzurenda, P. and Dobias, P., 2021, August. Implementing CRYSTALS-Dilithium signature scheme on FPGAs. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-11).

17. Sharath, H.A., Vrindavanam, J., Dana, S. and Prasad, S.N., 2025. Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms. IEEE Access. Available at https://www.academia.edu/download/121080605/Cyber_Security_Implications_of_Quantum_Computing_Shor_s_Algorithm_and_Beyond.pdf

18. Singh, C., Thakkar, R. and Warraich, J., 2023. IAM identity Access Management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), pp.30-38. Available at Available at https://www.ej-eng.org/index.php/ejeng/article/view/3074

19. Singh, C., Thakkar, R. and Warraich, J., 2023. IAM identity Access Management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), pp.30-38. Available at https://www.ej-eng.org/index.php/ejeng/article/view/3074

20. SS, A. and Devprasad, K.D., 2024. Enhancing security in Wireless Body Area Networks (WBANs) with ECC-based Diffie-Hellman Key Exchange algorithm (ECDH). Technology and Health Care, 32(6), pp.4765-4784. Available at https://journals.sagepub.com/doi/abs/10.3233/THC-231614

21. Tom, J.J., Anebo, N.P., Onyekwelu, B.A., Wilfred, A. and Eyo, R.E., 2023. Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol, 12(5), pp.25-38.. Available at https://www.researchgate.net/profile/Bukola-Onyekwelu/publication/371963926_Quantum_Computers_and_Algorithms_A_Threat_to_Classical_Cryptographic_Systems/links/64dcbda078e40b48bd4ec9d4/Quantum-Computers-and-Algorithms-A-Threat-to-Classical-Cryptographic-Systems.pdf

22. UZOKA, A.C., OGEAWUCHI, J.C., Abayomi, A.A., Agboola, O.A. and Gbenle, T.P., 2021. Advances in Cloud Security Practices Using IAM, Encryption, and Compliance Automation. Iconic Research and Engineering Journals, 5(5), pp.432-456. Available at https://www.researchgate.net/profile/Jeffrey-Ogeawuchi/publication/392708570_Advances_in_Cloud_Security_Practices_Using_IAM_Encryption_and_Compliance_Automation/links/684ee9db24267473b7776cab/Advances-in-Cloud-Security-Practices-Using-IAM-Encryption-and-Compliance-Automation.pdf

23. Vakarjuk, J., Snetkov, N. and Laud, P., 2024, May. Identifying Obstacles of PQC Migration in E-Estonia. In 2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon) (pp. 63-81). IEEE.

Available at https://ieeexplore.ieee.org/abstract/document/10685570/

24. Vyavahare, R.R., 2025. Exploring Hybrid Encryption for Enhanced Security of Electronic Health Record in Cloud Environment (Doctoral dissertation, Dublin, National College of Ireland). Available at https://norma.ncirl.ie/8063/

25. Wiesmaier, A., Alnahawi, N., Grasmeyer, T., Geißler, J., Zeier, A., Bauspieß, P. and Heinemann, A., 2021. On PQC migration and crypto-agility. arXiv preprint arXiv:2106.09599. Available at https://arxiv.org/abs/2106.09599

26. Zhou, Y. and Zhu, E., 2024. A new image encryption based on hybrid heterogeneous time-delay chaotic systems. AIMS Mathematics, 9(3), pp.5582-5608. Available at https://www.aimspress.com/aimspress-data/math/2024/3/PDF/math-09-03-270.pdf

References of Figure

1. Apriorit, 2022. Preparing Your Software for Post-Quantum Cryptography: A Practical Guide to Crypto-Agility. Available at https://www.apriorit.com/dev-blog/prepare-for-post-quantum-cryptography-with-crypto-agility

2. B. Ranganatha Rao, B. Sujatha, 2023. A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. Available at https://www.sciencedirect.com/science/article/pii/S2665917423002064

3. Darkreading, 2020. A Guide to the NIST Cybersecurity Framework. Available at https://www.darkreading.com/physical-security/a-guide-to-the-nist-cybersecurity-framework

4. Kaushik Mazumdar, 2024. State-of-the-art analysis of quantum cryptography: applications and future prospects. Available at https://www.frontiersin.org/journals/physics/articles/10.3389/fphy.2024.1456491/full

5. Sunil Kumar, 2025. HIPAA vs GDPR Compliance: A Guide for Businesses. Available at https://www.ailoitte.com/blog/hippa-vs-gdpr/

6. Swastik Kumar SahuKaushik Mazumdar

7. Umesh Kumar, 2024. Hybrid Cryptography: The Key to Secure Data In Cloud Computing. Available at https://www.google.com/url?sa=i&url=https%3A%2F%2Ftechbullion.com%2Fhybrid-cryptography-the-key-to-secure-data-in-cloud-computing%2F&psig=AOvVaw1xPg2H0vCZjpn8nLIK7SEy&ust=1759166905501000&source=images&cd=vfe&opi=89978449&ved=0CBgQjhxqFwoTCJiihcj9-48DFQAAAAAdAAAAABAy