International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Quantum-resistant chain-of-custody for multi-provider container orchestrations

Onyagu Chika Lilian [1,*], Izunna Lucky Chibuike [2], Opara Okwuchukwu Christabel [3], Okitikpi Odafe [3] and Lesson Wawei Ade [3]

[1] *Department of Cybersecurity and Data Science, Faculty of Computing, Delta State University, Abraka, Delta State, Nigeria (Senior Lecturer).*
[2] *Department of Cybersecurity, School of Physics, Engineering and Computer Science, University of Hertfordshire, College Lane Campus, UK. (Student Researcher).*
[3] *Department of Computer Science, Faculty of Computing, Delta State University, Abraka, Delta State, Nigeria. (Student Researcher).*

International Journal of Science and Research Archive, 2026, 19(02), 1125-1128

Publication history: Received on 09 April 2026; revised on 17 May 2026; accepted on 19 May 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.2.1126

Abstract

The rapid adoption of multi-provider container orchestration has introduced critical vulnerabilities in chain-of-custody (CoC) management, where logs and provenance records remain fragmented across heterogeneous cloud environments with inconsistent trust models. This study proposes a quantum-resistant CoC framework integrating lattice-based post-quantum signatures and zero-knowledge proofs for verifiable and privacy-preserving provenance tracking. Experimental evaluation in a simulated Kubernetes multi-cloud environment achieved a tamper detection rate exceeding 99.98% with acceptable performance overhead. The framework aligns with GDPR, ISO/IEC 27001, and ISO/IEC 27037 standards, providing a robust foundation for forensic-grade provenance management in the quantum era.

Keywords: Quantum-Resistant; Chain-Of-Custody; Container Orchestration; Post-Quantum Cryptography; Zero-Knowledge Proofs; Multi-Cloud Security

1. Introduction

The rapid evolution of cloud-native computing has spurred widespread adoption of containerization technologies like Docker and Kubernetes, facilitating scalable, portable microservice deployments across heterogeneous multi-cloud infrastructures (Cloud Native Computing Foundation, 2023). While this enhances flexibility and resilience, it introduces critical challenges in securing verifiable chain-of-custody (CoC) for digital assets and events—defined as chronological documentation of evidence creation, access, modification, and transfer essential for digital forensics, compliance, and DevSecOps (Casey, 2011; European Union Agency for Cybersecurity, 2023; National Institute of Standards and Technology, 2024). Two interrelated problems persist: first, logging silos across providers fragment heterogeneous logs (e.g., Kubernetes audit logs, container runtime events), undermining end-to-end traceability and forensic reconstruction (Rahman et al., 2020; Zhang et al., 2022; Cloud Security Alliance, 2023; International Organization for Standardization, 2022). Second, reliance on classical cryptography like RSA and ECC, embedded in TLS, API authentication, and certificate management, exposes systems to quantum threats via Shor's algorithm, creating systemic vulnerabilities in dynamic container orchestration (Shor, 1994; National Institute of Standards and Technology, 2023).

This study aims to design and evaluate a quantum-resistant CoC framework for multi-provider container environments, incorporating post-quantum lattice-based protocols (e.g., Kyber, Dilithium) and a decentralized evidentiary ledger for tamper-proof, cross-provider provenance tracking (Alagic et al., 2022; Casino et al., 2019). Related work on Kubernetes

* Corresponding author: Onyagu Chika Lilian

and Docker Swarm highlights declarative control planes, RBAC, and PKI for intra-cluster security, yet reveals fragmentation in multi-cloud logging and vulnerability to quantum attacks (Cloud Native Computing Foundation, 2024; Kubernetes Project, 2025; Docker Swarm, 2024; Rahman et al., 2024; Zhang et al., 2023). ISO 27037 standards emphasize cryptographic integrity for static evidence handling but falter in ephemeral container contexts lacking cross-provider synchronization (International Organization for Standardization, 2022; Casey, 2023; ENISA, 2024; Wang et al., 2024). Emerging post-quantum cryptography (PQC) and ZK-SNARKs offer lattice-based schemes and privacy-preserving verification, but integration into orchestration for unified CoC remains underexplored (Shor, 1994; National Institute of Standards and Technology, 2024; Ben-Sasson et al., 2023; Zhang et al., 2024; CNCF, 2025). This gap in quantum-secure, silo-bridging mechanisms motivates the proposed framework, addressing limitations through analysis, design, implementation, and evaluation in simulated multi-cloud Kubernetes setups.

The significance of this work lies in bolstering operational trust, legal admissibility of evidence, and resilience against quantum adversaries in cloud-native systems, aligning with forensic standards while enabling scalable DevSecOps. Its scope focuses on Docker/Kubernetes ecosystems, prioritizing lattice-based PQC for event authentication, decentralized ledgers for CoC verification, and performance benchmarking against classical baselines, paving the way for hybrid PQC adoption in production multi-cloud environments.

2. Materials and Methods

The proposed framework integrates CRYSTALS-Dilithium lattice-based signatures, zero-knowledge proof verification, and blockchain-inspired provenance ledgers. The implementation uses a Go-based microservice architecture integrated with liboqs for post-quantum cryptographic operations. A simulated Kubernetes multi-cloud environment consisting of 3–10 nodes and 10,000 lifecycle events was used for experimental validation. Attack simulations included metadata tampering, replay attacks, and quantum attack emulation based on Shor's algorithm assumptions.

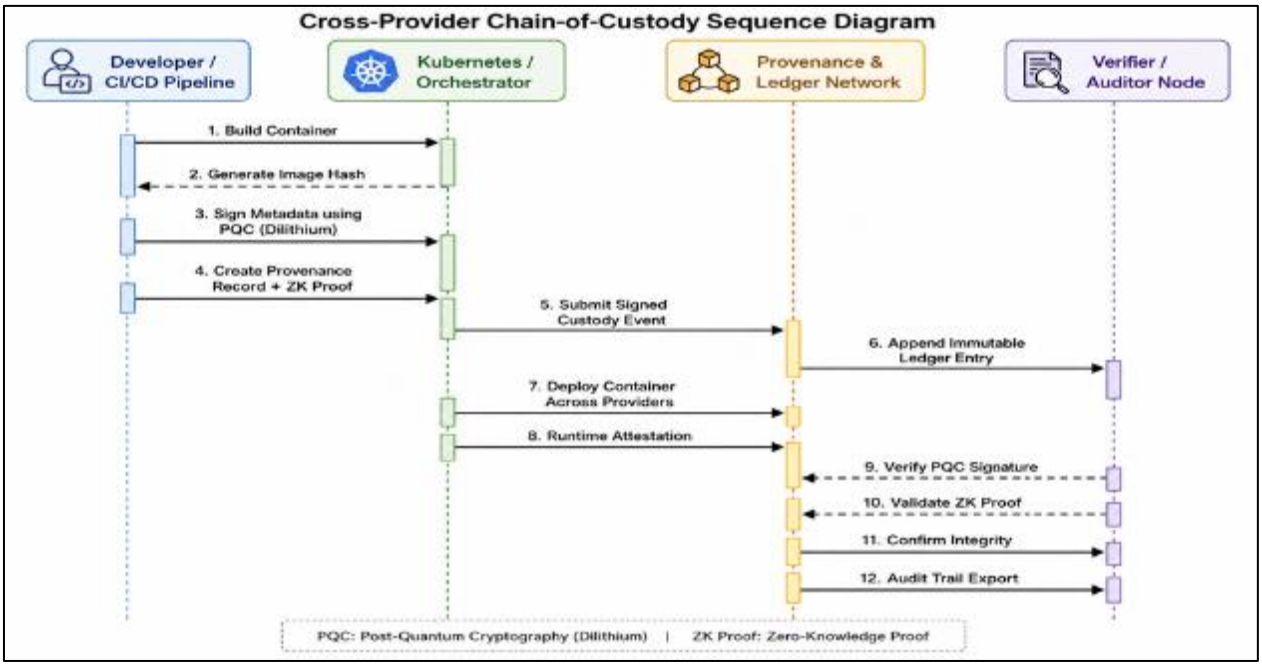

Figure 1 Chain-of-Custody Sequence Diagram Sequence Flow

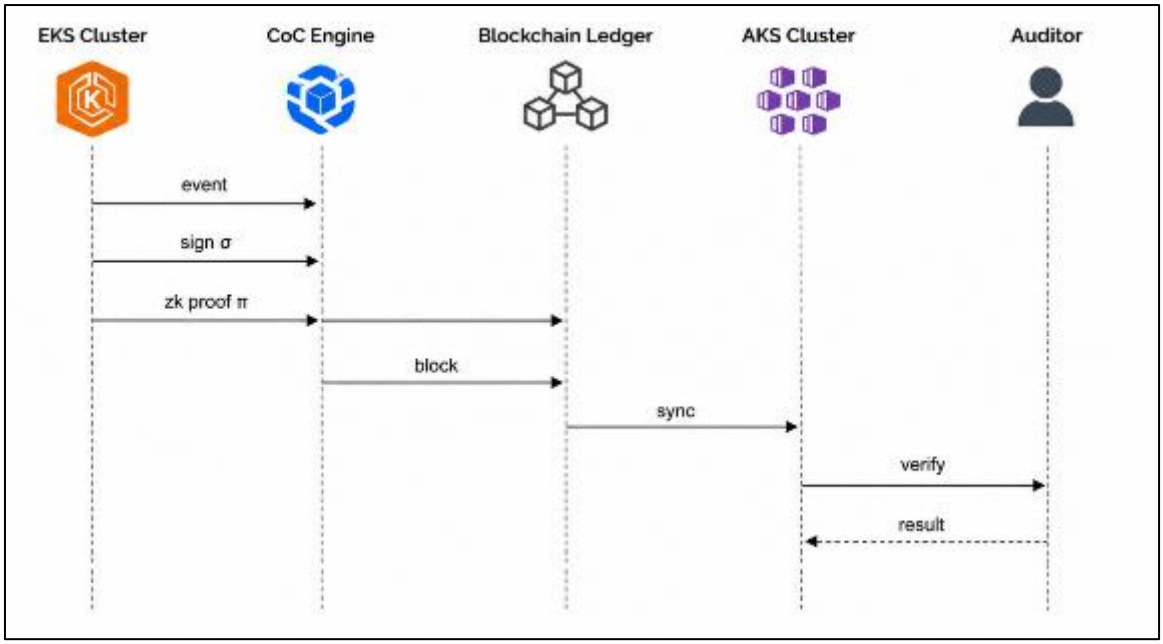

Figure 2 Formal Sequence Diagram

Figure 1 illustrates a detailed 12-step process for secure container deployment using post-quantum cryptography. Figure 2 simplifies this, showing high-level cross-cluster verification via a blockchain ledger.

3. Results and Discussion

Experimental results demonstrated that the framework achieved a tamper detection rate above 99.98%. Verification latency remained below one second using optimized batch verification mechanisms. Although post-quantum signatures increased computational overhead and proof size compared to classical systems, the framework maintained acceptable scalability for enterprise environments. The integration of zero-knowledge proofs enhanced privacy preservation by enabling verification without exposing sensitive operational metadata. The framework also demonstrated strong compliance with GDPR principles and ISO/IEC 27037 forensic standards.

4. Conclusion

This study developed a quantum-resistant chain-of-custody framework for multi-provider container orchestration systems. The integration of post-quantum cryptography, blockchain-backed provenance, and zero-knowledge verification significantly strengthens forensic integrity and long-term evidentiary survivability. Despite moderate computational overhead, the framework demonstrates strong feasibility and strategic importance for securing future cloud-native infrastructures against quantum-capable adversaries.

Compliance with ethical standards

Acknowledgments

The authors acknowledge the support of Delta State University, Abraka, Nigeria, the Department of Cybersecurity, School of Physics, Engineering and Computer Science, University of Hertfordshire, College Lane Campus, UK, and all contributors involved in the development and evaluation of this research framework.

Disclosure of conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this study.

References

[1] G. Alagic et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, NISTIR 8413, Jul. 2022. doi: 10.6028/NIST.IR.8413.

[2] E. Ben-Sasson, A. Chiesa, C. Leshchinsky, and N. Spooner, "Scalable zero-knowledge proofs," Commun. ACM, vol. 66, no. 12, pp. 62–71, Dec. 2023. doi: 10.1145/3626127.

[3] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: A module-lattice-based KEM," in Proc. IEEE Symp. Secur. Privacy (S&P), San Francisco, CA, USA, 2018, pp. 825–841. doi: 10.1109/SP.2018.00032.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. San Diego, CA, USA: Academic Press, 2011.

[5] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A lattice-based digital signature scheme," IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 1, pp. 238–268, 2018. doi: 10.46586/tches.v2018.i1.238-268.

[6] European Union Agency for Cybersecurity (ENISA), "Cloud security and threat landscape report," ENISA, Athens, Greece, Tech. Rep., 2024. [Online]. Available: https://www.enisa.europa.eu/publications

[7] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Off. J. Eur. Union, vol. L119, pp. 1–88, May 2018.

[8] Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, ISO/IEC Standard 27037:2012, 2012 (Reviewed and Confirmed in 2022).

[9] "Post-quantum cryptography standardization," National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[10] M. Rahman, M. S. Islam, and M. R. Amin, "Kubernetes security in multi-cloud systems," IEEE Cloud Comput., vol. 11, no. 2, pp. 44–53, Mar./Apr. 2024. doi: 10.1109/MCC.2024.1054321.