International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

Performance Characterization of Quantum-Safe Break-Glass Access for Electronic Medical Records

Vignesh L. S.[1], Dr. M Sathya[2], C Prathap[3], Dr. T Venishkumar[4], Vinothkumar[5], V Vinothini[6]
[1],[4]Department of Artificial Intelligence and Data Science, Nadar Saraswathi College of Engineering and Technology, Theni, India.
[2,6]Department of Computer Science and Engineering, Nadar Saraswathi College of Engineering and Technology, Theni, India.
[3]Department of Information Technology, Nadar Saraswathi College of Engineering and Technology, Theni, India.
[5]Department of Electronics and Communication Engineering, Nadar Saraswathi College of Engineering and Technology, Theni, India.
Email Id: *lsisreviving@gmail.com[1]*

Abstract
Migrating electronic medical records (EMRs) to post-quantum cryptography is urgent, because records exfiltrated today can be decrypted once a cryptographically relevant quantum computer exists. EMRs add a requirement generic data protection lack: regulated break-glass access, in which an unauthorized clinician opens a record during an emergency under mandatory accountability. PQ-BG is a break-glass EMR scheme built entirely from quantum-resistant components, AES-256-GCM, ML-KEM-768 (FIPS 203), Shamir (t, n) secret sharing, and an ML-DSA-65-signed (FIPS 204) hash-chained audit trail. A design alone, however, does not establish whether quantum-safe accountable emergency access is practical, or what it costs. This paper reports a seven-part empirical characterization on commodity clinical-workstation hardware. Record protection stays under 150 ms even for 200 MB DICOM studies; fully audited emergency access completes in 259 ms at a (3, 5) custodian configuration; per-record overhead is a constant 9.2 KB; and a single workstation sustains roughly 23 protections per second with linear scaling to 10,000 records. A classical RSA/ECDH baseline isolates migration cost. The decomposition shows that accountability signatures, not lattice key encapsulation, dominate emergency-path latency, redirecting where optimization belongs. All figures are conservative upper bounds from a Pure-Python backend.

Keywords: *break-glass access; electronic medical records; ML-DSA; ML-KEM; performance evaluation; post-quantum cryptography; Shamir secret sharing.*

1. Introduction
Medical records occupy a uniquely difficult position in information security: their confidentiality horizon, often the full lifetime of the patient and beyond, exceeds the expected security lifetime of the public-key algorithms that protect them. National standardization bodies project that cryptographically relevant quantum computers capable of executing Shor's algorithm against RSA and elliptic-curve cryptography may arrive within the coming decades, and adversaries need not wait: encrypted records exfiltrated today can simply be stored until decryption becomes feasible, the harvest-now-decrypt-later attack. NIST's finalization of the first post-quantum standards in August 2024, the module-lattice key-encapsulation mechanism ML-KEM (FIPS 203) and the module-lattice digital signature ML-DSA (FIPS 204), provides the primitives for a migration that, for healthcare, is therefore not optional but urgent [1], [2]. The research community has responded with a wave of quantum-resistant constructions for healthcare data: blockchain-anchored lattice threshold signcryption [3], quantum-key-based record sharing on distributed ledgers [4], hybrid classical/post-quantum multi-factor

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

authentication [5], post-quantum multi-factor protocols for medical IoT [6], and integrations of NIST primitives into blockchain platforms [7]. A common pattern unites these proposals: they compose multiple advanced mechanisms, distributed ledgers, signcryption, hybrid key agreements, into architecturally heavy systems whose deployment cost in a real hospital is substantial. Meanwhile, a requirement that is mandatory in clinical practice and codified in regulation has been left almost untouched by the post-quantum literature: emergency, or break-glass, access. When an unconscious patient arrives, a clinician who holds no authorization for that record must obtain it within seconds; regulations such as HIPAA accommodate this through emergency-access procedures, provided the access is fully accountable after the fact. PQ-BG was introduced as a deliberately minimal quantum-safe break-glass scheme: records are encrypted under fresh AES-256-GCM keys; routine access wraps each key with ML-KEM-768 (FIPS 203) [1]; emergency access splits the key via Shamir (t, n) secret sharing [8], whose security is information-theoretic; and every break-glass event appends an ML-DSA-65-signed (FIPS 204) [2], hash-chained audit entry before release. A companion paper specifies the construction and proves confidentiality, emergency availability, threshold secrecy, and tamper-evidence. What a design alone cannot settle is whether such a scheme is practical on the hardware hospitals already own, and what quantum safety costs relative to the classical primitives it replaces. This paper answers those questions empirically. We make four contributions. First, we benchmark the primitive costs and the record-protection pipeline across four orders of magnitude of record size, from 1 KB prescriptions to 200 MB imaging studies. Second, we measure end-to-end audited emergency latency across custodian configurations up to (5, 10) and decompose it, showing that the mandatory accountability signatures, not the lattice key recovery, set the latency budget. Third, we test batch scalability to 10,000 records and demonstrate audit-chain tamper detection. Fourth, we report a classical RSA/ECDH baseline that quantifies the cost of migration honestly, separating an implementation-language artifact from the intrinsic ciphertext expansion of the lattice setting. Section II recaps the PQ-BG construction and the post-quantum and break-glass literature that frames the measurements. Section III states the experimental methodology. Section IV reports the seven-part evaluation. Section V discusses where the latency goes and the limitations of a pure-Python characterization, and Section VI concludes.

2. Background And Related Work

2.1.The PQ-BG Scheme in Brief

The system comprises an EMR repository, authorized users each holding an ML-KEM-768 key pair, n custodians (organizationally independent hospital authorities) each holding an ML-KEM-768 key pair for share reception and an ML-DSA-65 key pair for audit signing, and an append-only audit log. The adversary is quantum-capable, may compromise the repository and up to t-1 custodians, and may record all ciphertexts for future decryption. For each record R with identifier rid, PQ-BG samples a fresh 256-bit data encryption key (DEK) and computes C = AES-256-GCM (DEK, R) with rid as associated data. Routine access wraps the DEK per authorized user through ML-KEM-768 encapsulation followed by an HKDF-derived AES-GCM wrap. Emergency access splits the DEK with Shamir secret sharing [8] over GF(2^8) into n shares with threshold t, wraps each share to one custodian, and, before any plaintext is released, appends an audit entry signed by every participating custodian with ML-DSA-65 and chained to the hash of the previous entry. Figure 1 shows the architecture.

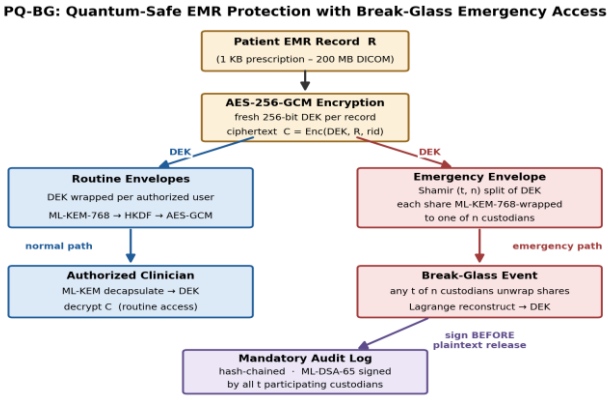

Figure 1 PQ-BG architecture: the normal path (left) and the emergency path (right) share a single AES-GCM data layer; the audit log is a mandatory waypoint of every break-glass event

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

As shown in Figure 1 PQ-BG architecture: the normal path (left) and the emergency path (right) share a single AES-GCM data layer; the audit log is a mandatory waypoint of every break-glass event Five security goals organize the scheme: (G1) record confidentiality against quantum adversaries; (G2) routine access exclusively for authorized users; (G3) emergency availability, any t of n custodians suffice; (G4) threshold secrecy, fewer than t custodians learn nothing about the DEK; and (G5) accountable, tamper-evident break-glass, no emergency access without a verifiable, signed, chained audit record. The evaluation that follows treats these as the properties whose cost must be paid; G5 in particular is the source of the dominant latency term reported in Section IV.

2.2.Post-Quantum Protection of Health Records

Lattice-based constructions dominate recent quantum-resistant healthcare proposals. The PQSHR scheme of Sourav and Ali combines lattice threshold ring signcryption with a blockchain layer, grounding security in the SIS and LWE problems with proofs in the random-oracle model [3]; the construction provides strong decentralized verifiability at the cost of considerable protocol machinery. Quantum-key-based sharing schemes anchor EMR exchange on distributed ledgers with smart-contract access control [4], presupposing quantum key infrastructure whose near-term hospital availability is doubtful, and quantum-secured blockchain frameworks generalize this direction to broader post-quantum data security [9]. Hybrid signature constructions combine ECDSA with Dilithium through lattice blind signatures to protect EHR integrity against quantum adversaries [10]. On the authentication side, Ahmad and Jagatheswari develop quantum-safe multi-factor authentication for cloud-assisted medical IoT [6] and a lattice three-party key agreement for medical gateways [11]; Braeken's framework flexibly composes ECC with a post-quantum KEM for bidirectional multi-factor authentication [5], representing the hybrid philosophy that hedges classical and post-quantum assumptions; and PQCAIE provides post-quantum authentication for IoT-based e-health over TLS 1.3 [12]. Revathi and Suganthi integrate NIST PQC algorithms into blockchain to harden ledger security [7]. Implementation work demonstrates feasibility on constrained platforms, notably a unified FPGA architecture executing both Dilithium and Kyber with shared resources [13], while certificateless lattice proxy re-signatures reduce delegation costs in IoT settings [14]. Surveys map post-quantum blockchain security for the IoT [15], the broader landscape of quantum threats to encryption and network protocols [16], and institutional migration frameworks [17]. None of these works addresses emergency access: the implicit assumption throughout is that the requesting party is authorized.

2.3.Break-Glass Access Control and Encryption

Classical break-glass research splits into cryptographic and accountability-oriented lines, and both remain active. On the cryptographic side, CP-ABE is the instrument of choice: revocable and verifiable weighted-attribute encryption supports collaborative multi-user access to cloud EHRs over bilinear pairing groups [18], and cross-hospital authentication schemes secure IoMT data exchange with classical three-factor constructions [19]. Accountability-first designs route emergency events through public blockchains, verifying the accessing clinician via self-sovereign identity while patients pre-authorize sharing scopes [20]; MedAccessX combines attribute- and role-based control on a permissioned ledger for dynamic IoMT access governance [21]; and policy-compliance frameworks formalize HIPAA-style obligations, logging, notification, and review, that any emergency-access mechanism must discharge [22]. The shared foundation of the cryptographic enforcement in all these schemes, bilinear pairings or elliptic-curve groups, is precisely what quantum computation invalidates, and the ledger-based designs additionally inherit multi-second consensus latencies on their critical path. To the best of our knowledge, and supported by the absence of any such proposal in recent surveys [15], [16], no break-glass construction from quantum-resistant assumptions has been published; PQ-BG fills this gap, and does so without attempting a lattice ABE analogue, which current evidence suggests is impractical, but by reducing emergency access to threshold secret sharing and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

standard KEM/signature primitives.

3. Experimental Methodology

All experiments ran on a commodity clinical-workstation-class machine: AMD Ryzen (Zen-3 family) under Windows 11 with CPython 3.14, representative of hospital desktop hardware rather than datacenter servers. PQ-BG was implemented over the kyber-py and dilithium-py reference libraries (pure Python) with AES-GCM, HKDF, and the classical baselines provided by OpenSSL through the cryptography package; Shamir sharing over GF(2^8) was implemented directly. Timings use a high-resolution monotonic counter with three warm-up iterations preceding each measured batch; we report mean, standard deviation, and median over the iteration counts stated per table. Two reporting conventions ensure fairness. First, because the post-quantum libraries are pure Python while the classical baseline is optimized C[19], all post-quantum timings constitute conservative upper bounds; optimized implementations such as liboqs reduce lattice operation costs by two to three orders of magnitude, so absolute PQ-BG latencies in production would be strictly lower than reported here. Second, every result row records [20] the producing backend, and the complete CSV outputs and source code accompany this paper as supplementary material for reproducibility as shown in Table 1 Primitive microbenchmarks (100 iterations each; Pure-Python lattice backend). Object sizes: ML-KEM-768 public key 1,184 B, ciphertext 1,088 B; ML-DSA-65 signature 3,309 B [21].

4. Results

4.1.Primitive Costs

Table 1 Primitive microbenchmarks (100 iterations each; Pure-Python lattice backend). Object sizes: ML-KEM-768 public key 1,184 B, ciphertext 1,088 B; ML-DSA-65 signature 3,309

Operation	Mean (ms)	SD (ms)	Median (ms)
ML-KEM-768 keygen	6.07	1.12	5.77
ML-KEM-768 encapsulation	8.09	1.06	7.75
ML-KEM-768 decapsulation	10.40	1.06	10.09
ML-DSA-65 keygen	16.89	1.00	16.65
ML-DSA-65 sign (256 B)	78.42	46.60	64.53
ML-DSA-65 verify	14.42	1.65	14.04
AES-256-GCM encrypt (1 MB)	0.56	0.11	0.50
AES-256-GCM decrypt (1 MB)	0.52	0.10	0.48

Two observations shape the rest of the evaluation. AES-GCM moves data at roughly 1.8 GB/s, so the symmetric layer is effectively free; and ML-DSA signing is both the most expensive primitive (mean 78.4 ms) and the most variable (SD 46.6 ms, maximum 213.9 ms), a direct consequence of the algorithm's rejection-sampling loop, whose iteration count is itself randomized. The high variance is intrinsic to the standard, not an artifact of our implementation, and reappears as the dominant term of emergency-path latency.

4.2.Record Protection Pipeline

Across four orders of magnitude of record size, 1 KB prescriptions, 100 KB lab reports, 5 MB image slices, and 50–200 MB DICOM studies, protection cost is nearly flat: 46.8 ms at 1 KB and 47.9 ms at 5 MB, rising only to 64.7 ms at 50 MB and 133.0 ms at 200 MB as bulk AES encryption finally becomes visible. The flat region confirms that the (u+n)=8 lattice envelopes, which are independent of record size, dominate small-record cost, while even the largest imaging study is protected well under 150 ms. Routine access is faster still, 7–10 ms for records up to 5 MB and 107 ms at 200 MB, since it performs a single decapsulation. Storage overhead is constant at 9,212 B per record: 0.9% of a 1 MB record and 0.004% of a 200 MB study, against 28 B for plain AES-GCM.As shown in Figure 3 Emergency-envelope costs across custodian configurations (t, n). Shamir costs are plotted ×100 for visibility.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

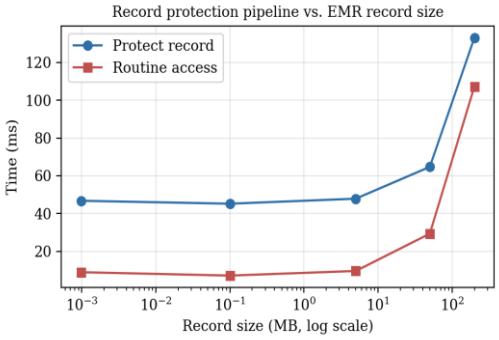

Figure 2 **Protection and routine-access latency versus record size (20 iterations; 5 for ≥50 MB)**

4.3.Emergency Envelope and Custodian Configurations

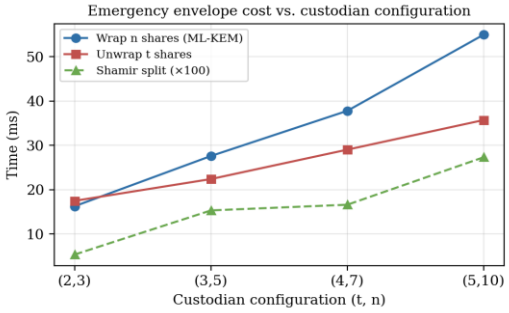

Figure 3 **Emergency-envelope costs across custodian configurations (t, n). Shamir costs are plotted ×100 for visibility**

The information-theoretic component is essentially free: splitting a 32-byte DEK costs 0.054–0.273 ms and reconstruction 0.054–0.260 ms across configurations from (2, 3) to (5, 10), three orders of magnitude below the lattice operations. Wrapping all n shares grows linearly from 16.3 ms (n=3) to 55.0 ms (n=10), and unwrapping t shares from 17.5 ms (t=2) to 35.7 ms (t=5). A hospital can therefore scale its custodian board generously, governance, not cryptography, should choose (t, n). A below-threshold sanity checks confirmed that t−1 shares fail to reconstruct the DEK.

4.4.End-to-End Break-Glass Latency

As shown in Figure 4 End-to-end emergency access latency: share unwrapping, reconstruction, mandatory signed audit, and record decryption (30 iterations)

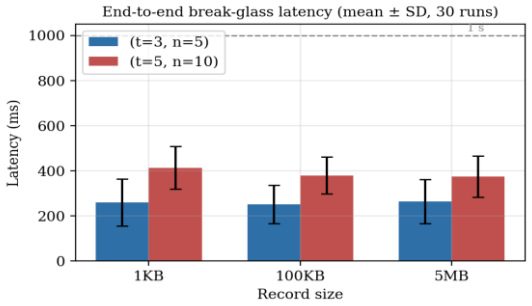

Figure 4 **End-to-end emergency access latency: share unwrapping, reconstruction, mandatory signed audit, and record decryption (30 iterations)**

Table 2 **Break-glass end-to-end latency (headline result)**

Config (t, n)	Record	Mean (ms)	Median (ms)	Max (ms)
(3, 5)	1 KB	259.4	235.2	542.4
(3, 5)	100 KB	252.1	230.8	434.1
(3, 5)	5 MB	265.3	245.3	596.8
(5, 10)	1 KB	414.2	414.1	608.9
(5, 10)	100 KB	380.2	379.6	535.9
(5, 10)	5 MB	375.5	361.7	570.8

The headline result: complete, fully audited emergency access takes 259 ms on average at (3, 5) and 414 ms at (5, 10), with the worst case ever observed across 180 runs remaining below 0.61 s. Against clinical emergency workflows measured in minutes, and against blockchain-mediated emergency-access frameworks whose critical path includes ledger consensus and smart-contract execution [20], [21], sub-second cryptographic emergency access is operationally negligible, and this on an unoptimized interpreter. Latency is insensitive to record size (the AES layer contributes under 3 ms even at 5 MB) and grows sublinearly in t, because its dominant term is the t parallelizable ML-DSA audit signatures: at (3, 5), three signatures at a mean 78.4 ms each account for ≈235 ms of the 259 ms total, matching the median almost exactly. The break-glass bottleneck is thus accountability, not key recovery, a finding we return to in Section V.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

4.5.Audit Chain and Tamper Detection

Appending one audit event with three custodian signatures costs 228.4 ms (consistent with the signature decomposition above); verifying chains of 10, 50, and 100 entries costs 0.39 s, 2.05 s, and 4.00 s respectively, i.e., a clean 40 ms per entry, dominated by 3 ML-DSA verifications, making even a year of daily emergency events verifiable in seconds during a periodic compliance review. Both attack demonstrations succeeded: modifying the invoking-doctor field of entry 5 in a 10-entry chain and deleting that entry outright were each detected by chain verification, empirically confirming property G5, Figure 5 Batch protection of 10,000 records: strictly linear scaling at ≈23 records/s on one workstation (Pure-Python backend).

4.6.Scalability and Classical Baseline

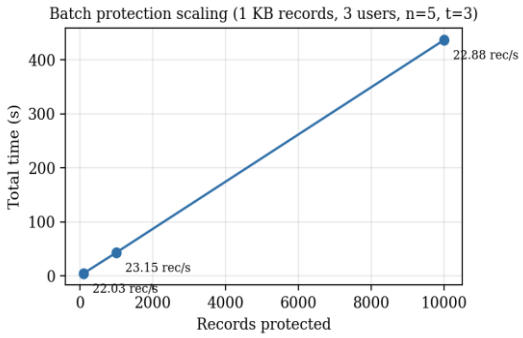

Figure 5 Batch protection of 10,000 records: strictly linear scaling at ≈23 records/s on one workstation (Pure-Python backend)

Protecting 100, 1,000, and 10,000 one-kilobyte records took 4.5 s, 43.2 s, and 437.1 s, a constant 22–23 records per second with no degradation across two orders of magnitude, so a one-time migration of a million-record archive would occupy a single workstation for roughly 12 hours, or proportionally less with optimized libraries and parallel cores. The classical baseline (Table III) quantifies the migration cost honestly: OpenSSL's C implementations of RSA-2048-OAEP and ECDH-P256 wrap a DEK in 0.038 ms and 0.115 ms respectively, versus 8.09 ms for Pure-Python ML-KEM-768, and an RSA-wrapped DEK occupies 256 B versus the 1,088 B ML-KEM ciphertext. The timing gap is overwhelmingly an implementation-language artifact, optimized ML-KEM implementations encapsulate in tens of microseconds, but the ≈4× ciphertext expansion is intrinsic to the lattice setting and is precisely the constant 9.2 KB per-record overhead already shown to be negligible against medical payloads. The security gap, conversely, is absolute: both baselines fall to Shor's algorithm, and both are scheduled for deprecation under announced national migration timelines [17].

Table 3 Classical (OpenSSL C) versus post-quantum (Pure-Python) DEK wrapping. The timing comparison is conservative against PQ-BG; the size comparison is intrinsic

Operation	Mean (ms)	SD (ms)	Size (B)
RSA-2048-OAEP wrap DEK	0.038	0.014	256
RSA-2048-OAEP unwrap DEK	0.701	0.145	n/a
ECDH-P256 wrap DEK (eph.+HKDF+GCM)	0.115	0.026	n/a
ECDH-P256 unwrap DEK	0.076	0.024	n/a
ML-KEM-768 encaps (pure Python)	8.09	1.06	1,088

5. Discussion and Limitations

Where the time goes. The decomposition of Section IV-D carries a design lesson that generalizes beyond PQ-BG: in accountable post-quantum systems, signature generation, not key encapsulation, is the latency budget. ML-DSA's rejection sampling makes its cost both high and variable, so systems that sign on the critical path, as any non-by passable audit must, should consider signing in parallel across custodians (reducing the t-signature term to a single signature latency), or precomputing signature randomness. Conversely, attempts to optimize the KEM or the secret sharing would be effort misplaced: Shamir operations cost microseconds. Limitations. First, our timings are upper bounds from a Pure-Python reference implementation; while this strengthens the feasibility claim, the headline is

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4854-4861
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0638

already sub-second, it means absolute values should not be compared across papers without normalizing for implementation language, and our classical baseline comparison is correspondingly framed around sizes rather than speed. Second, the comparison with classical pairing-based CP-ABE schemes [18] is qualitative and size-based, since pairing libraries are impractical on our Windows evaluation platform; a same-platform quantitative comparison is future work. Third, PQ-BG assumes threshold non-collusion among custodians and does not address custodian key loss, share refresh (proactive secret sharing would bolt on naturally, since shares are just bytes), or the orthogonal problem of re-encrypting archives when algorithms are deprecated, which we identify as the necessary companion problem for lifetime-scale EMR confidentiality. Fourth, endpoint compromise during the plaintext-handling window and side channels are out of scope, as in the classical break-glass literature.

Conclusion

Quantum-safe, accountable emergency access for electronic medical records is not only constructible but practical on the hardware hospitals already own. Across a seven-part evaluation, record protection stayed under 150 ms even for 200 MB imaging studies, fully audited break-glass completed in roughly a quarter second at a (3, 5) custodian board, per-record overhead held constant at 9.2 KB, and a single workstation protected tens of thousands of records per hour with strictly linear scaling, every number a conservative upper bound from an unoptimized pure-Python backend. The measurements also localize the cost: the accountability signatures, not the lattice key encapsulation or the information-theoretic secret sharing, dominate the emergency path, which redirects optimization effort for any non-bypassable post-quantum audit. Future work will repeat the characterization on an optimized backend such as liboqs, add proactive share refresh and a lifecycle re-encryption protocol for algorithm deprecation, and integrate the scheme with an open EMR platform via FHIR.

Acknowledgment

Data Availability

Data Availability. The reference implementation, benchmark harness, and the complete per-run CSV outputs underlying every figure and table accompany this paper as supplementary material and are available from the corresponding author on reasonable request.

Ethics Statement

Ethics Statement. This work uses no human subjects, animal models, or real patient data; all records are synthetic payloads generated for benchmarking.

Funding and Conflicts of Interest

Funding and Conflicts of Interest. This work received no external funding. The authors declare no competing interests.

References

[1]. National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[2]. National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS 204, Aug. 2024, doi: 10.6028/NIST.FIPS.204.

[3]. Sourav and R. Ali, "Post-quantum secure health records: a blockchain-based lattice threshold signcryption scheme," Cluster Computing, 2025, doi: 10.1007/s10586-025-05117-2.

[4]. D. Zhu, H. Zhou, Z. Zhou, et al., "Quantum key-based medical privacy protection and sharing scheme on blockchain," Scientific Reports, vol. 15, art. 27983, 2025, doi: 10.1038/s41598-025-10832-2.

[5]. A. Braeken, "Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ECC and KEM," Future Generation Computer Systems, vol. 166, 2025, doi: 10.1016/j.future.2024.107634.

[6]. A. Ahmad and S. Jagatheswari, "Quantum safe multi-factor user authentication protocol for cloud-assisted medical IoT," IEEE Access, vol. 13, pp. 3532–3545, 2025, doi: 10.1109/ACCESS.2024.3523530.

[7]. K. Revathi and K. Suganthi, "Enhancing blockchain security against quantum threats through integration of post-quantum

cryptographic algorithms," Computers and Electrical Engineering, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0045790625005531

[8]. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[9]. N. R. Reddy, S. Suryadevara, K. G. R. Reddy, R. Umamaheswari, R. Guttula, and R. Kotoju, "Quantum secured blockchain framework for enhancing post quantum data security," Scientific Reports, vol. 15, art. 31048, 2025, doi: 10.1038/s41598-025-16315-8.

[10]. S. Alsubai, A. Alqahtani, H. Garg, M. Sha, and A. Gumaei, "A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records," Complex & Intelligent Systems, 2024, doi: 10.1007/s40747-024-01477-1.

[11]. A. Ahmad and S. Jagatheswari, "Lattice-based three party authenticated key agreement scheme in medical IoT for post-quantum environment," IEEE Access, vol. 12, pp. 157247–157259, 2024, doi: 10.1109/ACCESS.2024.3483971.

[12]. K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," Internet of Things, vol. 27, art. 101228, 2024, doi: 10.1016/j.iot.2024.101228.

[13]. P. Dobias, L. Malina, and J. Hajny, "Efficient unified architecture for post-quantum cryptography: combining Dilithium and Kyber," PeerJ Computer Science, 2025, doi: 10.7717/peerj-cs.2746.

[14]. Z. Wei, G. Lan, H. Zhao, Z. Li, and Z. Ju, "Lattice-based certificateless proxy re-signature for IoT: a computation-and-storage optimized post-quantum scheme," Sensors, vol. 25, no. 15, art. 4848, 2025, doi: 10.3390/s25154848.

[15]. H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: survey and research directions," IEEE Communications Surveys & Tutorials, vol. 26, no. 3, pp. 1748–1774, 2024, doi: 10.1109/COMST.2024.3355222.

[16]. J. Ahn, R. Hussain, K. Kang, and J. Son, "Exploring encryption algorithms and network protocols: a comprehensive survey of threats and vulnerabilities," IEEE Communications Surveys & Tutorials, vol. 27, no. 6, 2025, doi: 10.1109/COMST.2025.3526605.

[17]. M. El Bizri, A. M. El-Hajj, L. Sliman, and A. M. Haidar, "Institutional approaches to post-quantum cryptography: a comparative analysis of migration frameworks," IEEE Access, vol. 14, 2026, doi: 10.1109/ACCESS.2025.3650465.

[18]. X. Li, H. Wang, S. Ma, M. Xiao, and Q. Huang, "Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud," Cybersecurity, vol. 7, no. 1, pp. 1–19, 2024, doi: 10.1186/s42400-024-00211-1.

[19]. Q. Xie and Z. Ding, "Provably secure and lightweight blockchain based cross hospital authentication scheme for IoMT-based healthcare," Scientific Reports, vol. 15, 2025, doi: 10.1038/s41598-025-90219-5.

[20]. T. Takahashi, Y. Zhihao, and K. Omote, "Emergency medical access control system based on public blockchain," Journal of Medical Systems, vol. 48, art. 90, 2024, doi: 10.1007/s10916-024-02102-x.

[21]. G. Shi, M. Qi, Q. Zhong, N. Li, W. Gao, L. Zhang, and L. Gao, "MedAccessX: A blockchain-enabled dynamic access control framework for IoMT networks," Sensors, vol. 25, no. 6, art. 1857, 2025, doi: 10.3390/s25061857.

[22]. M. Al Amin, R. Shah, F. Ahamed, et al., "A policy compliance framework for protected health information (PHI) emergency access," in Proc. 22nd Int. Conf. on Security and Cryptography (SECRYPT), 2025, doi: 10.5220/0013527000003979.