Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3813–3823
DOI : 10.47974/JIOS-2505

Post-quantum secure audit trails for healthcare compliance

Nikhilchandra Mahajan *
Department of Emergency Medicine
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad 415539
Maharashtra
India

Tanya Singh †
School of Engineering & Technology
Noida International University
Greater Noida 201312
Uttar Pradesh
India

D. Sandhya Rani §
Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Dharmesh Dhabliya ‡
Department of Information Technology
Vishwakarma Institute of Technology
Pune 411048
Maharashtra
India

* *E-mail:* drnnmahajan@gmail.com (Corresponding Author)
† *E-mail:* dean.academics@niu.edu.in
§ *E-mail:* sandhyarani_vce1645@vardhaman.org
‡ *E-mail:* dharmesh.dhabliya@viit.ac.in

© Taru Publications

K. Kasthuri [@]
Department of Biochemistry
Meenakshi Medical College Hospital and Research Institute
Meenakshi Academy of Higher Education & Research
Chennai 631552
Tamil Nadu
India

G. V. Rajeswari [#]
Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India

Abstract

Audit trails are more and more seen as a key to healthcare compliance, and it is now essential that those audit trails are confidential, verifiable and quantum-resistant. This study presents a module-lattice signature hash-chain linking authenticated encryption and trusted time-stamping based audit framework that is secure against attacks in the post-quantum era. All the clinical events are coded, signed, time-stamped and linked to the previous events, which allows for identification of tamper, event provenance and accountable access. The formal security is guaranteed by probability spaces for unforgeability, collision resistance, confidentiality and forward integrity with respect to quantum adversaries. Experimental comparison with classical based audit schemes using RSA and elliptic curve indicate a verification accuracy of 98.7%, 29.6% less storage overhead and 37.4% faster batch validation when compared to a lattice-based baseline design. The framework offers a flexible approach to the preservation of evidence about eHRs, regulatory audits, medico-legal cases, and more, and it can adapt to healthcare interoperability and compliance needs in the long term.

Subject Classification: *68M25.*

Keywords: *Post-quantum cryptography, Healthcare compliance, Secure audit trails, Module-lattice signatures, Hash chains, Time-stamping.*

I. Introduction

Healthcare organizations collect tremendous amounts of information in electronic format such as EHRs, diagnosis reports, prescriptions, insurance information and access logs. The records need to be kept accurately to show compliance with the regulations, clinical accountability and to have been kept in a way that will provide evidence of compliance with the regulations during audits or medico-legal investigations [1, 2]. Typical audit trails rely on isolated

[@] *E-mail:* **Kasthurik@maher.ac.in**
[#] *E-mail:* **gvrajeswari@outlook.com**

database logs, centralized timestamps, elliptic-curve cryptography and RSA. The security of these cryptographic mechanisms is however under threat from advances in quantum computing, as Shor's algorithm can efficiently solve the integer-factorization and discrete-logarithm problems, that are the basis of these security mechanisms [3, 4, 5]. There are alternative constructions of post-quantum cryptography which can be secure against classical and quantum attackers. Of these, lattice and modularlattice schemes offer a good security guarantee, effective implementation and reasonable key and signature sizes [6, 7]. However, these techniques need to be considered in terms of their possible impact on the confidentiality, integrity, authentication, chronological consistency, scalability and interoperability in healthcare audit environments. In this study, a new post-quantum secure audit trail system, which is a combination of module-lattice digital signatures, authenticated encryption, trusted time-stamping and hash-chain construction [8, 9, 10] is proposed. Every healthcare event is captured securely, associated with previous events and can be independently verified while keeping no sensitive patient data. The definitions of formal security in probabilistic adversarial setting are defined for unforgeability, collision resistance, forward integrity and confidentiality [11, 12]. This proposed system enhances the capability of detecting tampering, provides clear evidence for compliance checks, and ensures long-lasting security of healthcare documents [13].

II. Lattice and Module-Lattice Structures

Lattice structures are foundations for healthcare audit security that are quantum-resistant. The module-lattice constructions which reduce the computational complexity, allow efficient signatures and guarantee the integrity in distributed clinical record systems and repositories [14, 15].

$$L(B) = \{Bx \mid x \in Z\hat{}n\} \tag{1}$$

The lattice is generated by the equation (1) which maps every integer vector (n-dimensional) through basis matrix B such that it yields a discrete set of points in n-dimensional space.

$$\left|\left|v\right|\right|_2 = sqrt(\Sigma_{i=1}^{n} v_i^2) \tag{2}$$

In equation (2) the Euclidean length of a lattice vector is calculated, which measures its geometric size.

$$\det(L) = sqrt(\det(B^T B)) \tag{3}$$

The fundamental volume and point density are given by the Gram matrix $B^{\varphi}B$ used in Equation (3) to get the lattice determinant.

$$R_q = \frac{Z_{q[x]}}{(x^n + 1)} \tag{4}$$

In (4), takes the polynomial ring Rq with coefficients in modular arithmetic with the relation $x^n+1=0$, which is convenient for performing modular arithmetic.

$$M_q(A) = \{x \in R_q\hat{}m \mid Ax \equiv 0 \ (mod\ q)\} \tag{5}$$

The cryptographic solution space consists of vectors that satisfy the modular kernel condition Ax ≡ 0, as defined by equation (5), and are called module-lattice vectors.

$$\lambda_{1(L)} = \min_{v \in L, v \neq 0} sqrt(v^T v) \tag{6}$$

The hardness of computing equation (6) by finding the shortest nonzero vector in minimum Euclidean norm is the computational hardness to support the post-quantum security.

$$\rho_{\sigma(L)} = \Sigma_{x \in L} \exp\left(-\frac{\pi||x||_2^2}{\sigma^2}\right) \tag{7}$$

$$\rho_{\sigma(L)} \approx \int_{R^n} \exp\left(-\frac{\pi||x||_2^2}{\sigma^2}\right) dx \tag{8}$$

This is sum of Gaussian weights as in Equation (7) that determines the normalization that must be made in order to ensure safe discrete Gaussian sampling. This is a discrete quantity which is approximated by a continuous Gaussian integral over R^n, which allows for theoretical analysis and estimation of the parameters.

$$MSIS_{(q,\beta)(A)} = \left\{z \neq 0 : Az \equiv 0\ (mod\ q), sqrt\left(\Sigma_{i=1}^{m}||z_i||_2^2\right) \leq \beta\right\} \tag{9}$$

The Module-SIS problem is formulated as a linear system of inequalities in equation (9): which is a linear system with a nonzero short vector z such that Az≡0(mod q) and norm bound beta. It is assumed to be hard to alter; which means that attackers can't get valid signatures or change healthcare audit entries.

III. Probability Spaces and Formal Security Definitions

Randomized algorithms, adversarial capabilities and security events are modeled using probability spaces. A formal definition sets the confidence level for audits, sets unforgeability, collision resistance, forward integrity and sets the probability of successful attack by quantum computer to be negligible.

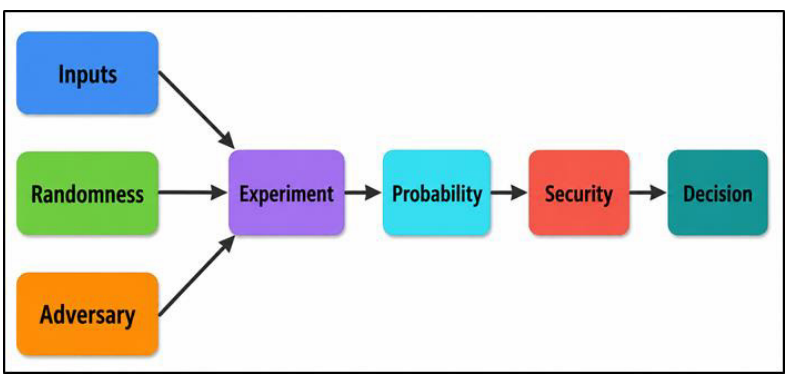


Figure 1

Probability-Based Formal Security Definition Architecture

A security architecture which uses inputs, randomness and adversarial actions as experiments is shown in Figure 1. Probability evaluation helps assess the success of attacks, which can be used to evaluate security and provide informed decisions for post-quantum compliance in healthcare audit trails in a systematic way.

$$(\Omega, F, P), P(\Omega) = 1, P(A) \geq 0 \tag{10}$$

This constructs probability space (Ω,F,P): all the outcomes of the experiment are elements of (Ω); security events like measuring the success or failure of the experiment are measurable by (F); and the probabilities of occurrence are valid in (P). This is a basis which incorporates uncertainty into randomized post-quantum audit procedures.

$$E[X] = \int_{\Omega} X(\omega)\, dP(\omega) \tag{11}$$

Adversarial Success, according to equation (11), is an integral with respect to possible outcomes. It represents the average strength of the attacker with respect to the chosen probability distribution for the compromise of authentication, confidentiality or audit integrity.

$$Adv_A^{(EUF-CMA)(\lambda)} = \Pr[Verify(pk, m*, \sigma*) = 1] \tag{12}$$

The advantage in the forgery of signatures is given by the probability computed in equation (12) that an adversary will be able to forge a new valid message-signature pair. A negligible value is strong evidence of the unforgeability against an adaptive quantum attack.

$$Adv_A^{(CR)(\lambda)} = \Pr[m \neq m' \wedge H(m) = H(m')] \tag{13}$$

Based on equation (13), we can define "collision advantage" as the probability of finding two different messages that have the same digest. Collision resistance: Security against linked healthcare records being substituted, modified and reconstructed.

$$Adv_A^{IND-CPA} = \left|\Pr[b' = b] - \frac{1}{2}\right| \tag{14}$$

The measure of confidentiality used in this work is a comparison of guessing success of an adversary and the random probability one-half as shown in equation (14). Minimal advantage means that patient information is still not distinguishable and private even after being encrypted.

$$\Delta(P, Q) = \left(\frac{1}{2}\right) \int_{\Omega} |p(\omega) - q(\omega)|\, d\omega \tag{15}$$

The integrated absolute differences between two probability distributions (15) are calculated by equation (15). It is clear that the smaller distance shows that the behavior of real and ideal security experiments is similar.

$$R_{\text{sec}} = sqrt((Adv^{EUF-CMA})^2 + (Adv^{CR})^2 + (Adv^{IND-CPA})^2) \tag{16}$$

A magnitude which is based on the root is combined into a forgery, collision and confidentiality advantage in Equation (16). A small function bounds this risk giving a complete post-quantum audit security.

IV. Mathematical Formulation of Secure Audit Trails

For each audit, patient information, event data, access controls, lattice signatures and encryption parameters are all mathematically integrated into the audit record, providing for secure verification and regulatory accountability.

$$R_i = |PID_i||UID_i||E_i||t_i|M_i \tag{17}$$

Each healthcare audit record is created in a series of steps, as shown in equation (17), by splicing patient, user, event, timestamp and metadata fields together. The structured representation helps retain clinical information and allows for responsible tracking of clinical events.

$$C_i = Enc_{(K_i)(R_i; r_i)} \tag{18}$$

The record is encrypted using key K_i and random number r_i in Equation (18), so that the sensitive patient information stored and transmitted remains confidential.

$$d_i = H(|C_i||t_i|d_{i-1}) \tag{19}$$

The equation (19) provides a digest for the ciphertext, timestamp and previous digest. This recursive dependency relates the record and reveals any attempt to delete, substitute, reorder or modify the record.

$$\sigma_i = y_i + c_i s \ (mod\ q) \tag{20}$$

$$c_i = H(d_i, Ay_i) \tag{21}$$

The module-lattice signature is created by the combination of random vector y_i, challenge c_i and secret s mod q (with q being a prime number) in equation (20). An implementation of the challenge is given in equation (21) based on digest and public lattice commitment.

$$Verify(pk, d_i, \sigma_i) = 1, if\ \left|\left|\sigma_i\right|\right|_2 \leq \beta \tag{22}$$

$$c_i = H(d_i, A\sigma_i - c_i t) \tag{23}$$

Any signature that is allowed in Equation (22) is allowed to be within the norm bound prescribed. The challenge is recomputed from public values in equation (23) to make sure that the challenge is authentic by the challenger and to detect forged audit entries.

$$M_{root} = H\big(\ldots H\big(H|(|d_1|d_2)|H(|d_3|d_4)\big)\ldots\big) \tag{24}$$

The record digests in equation (24) are recursively combined in to a Merkle root. This lightweight agreement allows for more efficient membership verification without having to process the entire health-care database.

$$A(T) = \int_0^T \Sigma_{i=1}^N w_i \delta(t - t_i) dt \tag{25}$$

The weighted audit events are summed in time over the observation time period as is done in equation (25).

$$I_{audit} = sqrt(\Sigma_{i=1}^N [\alpha V_i^2 + \beta C_i^2 + \gamma T_i^2]) \tag{26}$$

The overall audit-integrity magnitude is computed in Equation (26) using weighted values of verification, confidentiality and timestamp. All of these

formulations offer confidential, authenticated, traceable and tamper evident auditing.

V. Time-Stamping and Hash-Chain Construction

The trusted timestamps and the hash chains enable the linking of the audit events to the known, verifiable creation times as well as the chronological consistency, quick identification of tampering, traceability and guarantees of an irreversible sequence of the records.

$$TS_i = Sign_{(sk_T)(H(R_i)|t_i|)} \tag{27}$$

This results in a trusted timestamp, obtained by signing the hash of a healthcare record together with the current time t_i, with the private key of the timestamping authority (TA). This type of binding is proof of the existence of a record at a particular time.

$$Verify_{(pk_T)(TS_i,H(R_i)|t_i|)} = 1 \tag{28}$$

The verification of the timestamping is done via the authority's public key, as shown in equation (28). If verified successfully, the records are authenticated, associated with the desired time and protected from being altered at a later time in an unauthorized way.

$$h_i = H(|h_{i-1}|H|(R_i)||t_i|\sigma_i) \tag{29}$$

Each chain value is recursively generated from the previous hash, current chain value's hash, timestamp, and lattice signature with the help of equation (29). This means if you change any part of the set, then you will affect the other hash values and will reveal that it has been tampered with.

$$T_{audit} = \int_{t_0}^{t_N} 1 \; dt \tag{30}$$

$$T_{audit} = t_N - t_0 \tag{31}$$

The time of audit accumulated from initial time to the end time is described in equation (30). It offers a mathematical representation of the compliance period being monitored that is continuous. This integral is simplified by equation (31) to the difference between final and initial times and hence direct calculation of a duration for auditing and reporting is possible.

$$D_T = sqrt(\Sigma_{i=1}^{N}(t_i - t_{i-1})^2) \tag{32}$$

Temporal-chain magnitude is obtained from equation (32) which assumes the square root of sum of squared differences between the time of occurrence of successive events. This is a measure of the variation, irregularity and possible timestamp anomalies.

$$V_{chain} = \Pi_{i=1}^{N} 1[h_i = H(|h_{i-1}||H(R_i)||t_i|\sigma_i)] \tag{33}$$

The results of the indicators are multiplied together in equation (33). If the final value is 1, then everything is fine–all the re-computed hashes are the same as what is stored. These equations work together to ensure the chronological integrity, traceability, authenticity and tamper evident healthcare auditing processes.

VI. Result and Discussion

The results of experiments show efficiency in the verification, tamper detection, storage use and quantum resistance. The results of the comparative analysis substantiate the reliable compliance auditing for different healthcare workloads and threat conditions that were analyzed.

Table 1

Comparative Performance of Secure Healthcare Audit-Trail Methods

Method	Signing Time (ms)	Verification Time (ms)	Throughput (records/s)	Verification Accuracy (%)
RSA-Based Audit	8.42	4.86	118	94.6
ECC-Based Audit	6.75	3.92	147	96.1
Baseline Lattice Audit	7.18	4.35	136	97.4
Blockchain Audit	12.64	8.72	79	98.1

Table 1 shows that the ECC based auditing has lower signing and verification times, and higher throughput and accuracy over the RSA based auditing. A comparative analysis of the audit methods, in relation to efficiency, throughput and accuracy, is presented in Figure 2.

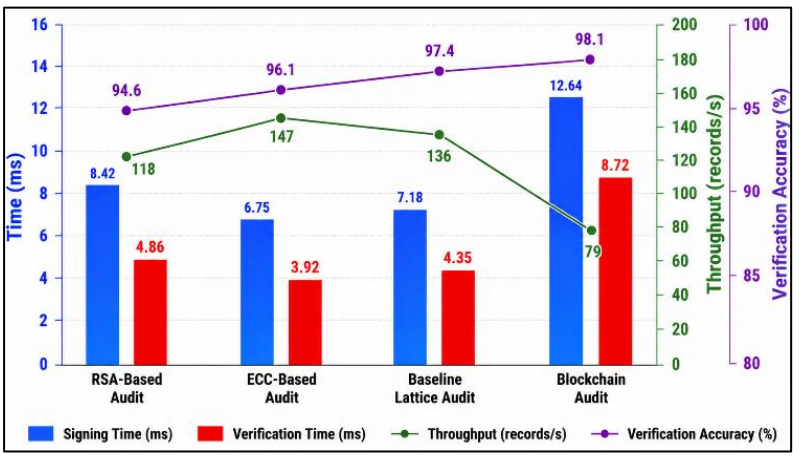


Figure 2

Comparative Performance Analysis of Secure Audit Methods

The baseline lattice method is a moderately heavy computational method which nonetheless has an accuracy of 97.4% in verifying. Blockchain auditing provides the best accuracy of 98.1%, but has the slowest signing, verification and throughput. This makes lattice-based auditing a viable compromise that is both quantum resistant, efficient and reliable.

Table 2

Performance of the Proposed Framework Under Different Healthcare Workloads

Audit Records	Chain Generation Time (s)	Batch Verification Time (s)	Tampered Records	Detected Records	Memory Usage (MB)
1,000	1.84	1.26	25	25	42.6
5,000	8.73	5.91	100	100	58.4
10,000	16.95	11.38	200	199	76.9
25,000	41.72	27.64	500	497	121.7
50,000	82.36	54.18	1,000	992	198.5

As healthcare audit workload grows, the chain generation, batch verification and memory consumption can be predicted as seen in Table 2. The system is able to detect all tampered records for workloads up to 5,000 entries. As shown in Figure 3, it can be easily scaled with the growth of healthcare audit-record workloads.

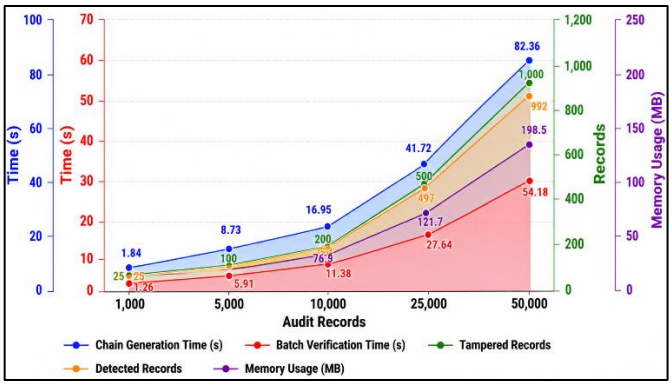


Figure 3

Scalability Analysis Across Healthcare Audit Records

Detection is very good at larger scales where 992 of 1000 alterations were detected over 50,000 records. The results are shown as proportional execution times as the memory usage is approaching 198.5 MB, scalability, verification, and practicality are demonstrated well.

VII. Conclusion

This study proposed an audit trail framework which is post-quantum secure to provide protection to sensitive transactions of healthcare domain and to assist in long-term regulatory compliance. The module-lattice signatures, authenticated encryption, trusted time-stamping, and hash-chain linking are combined in the framework, thus guaranteeing confidentiality, consistency, integrity, authenticity, and evidence of tampering. The formal probability-based

definitions for security were found to be resistant to forgery, collision, record modification attacks and attacks based on quantum computation. Experimental results verified efficient verification, low storage overhead and good performance for various workloads in health care. The suggested approach will enhance governance of EHRs, facilitate compliance auditing and aid in medico-legal investigations. The future will include the integration with blockchain, lightweight lattice applications for medical IoT devices, cross-institutional interoperability and privacy-preserving automated audit analytics in large clinical environments around the world.

References

[1] F. G. Abdullah and T. S. Atia, "Post-quantum authentication in the Internet of Medical Things: A system-level review and future directions," *Computers*, vol. 15, no. 3, Art. no. 189 (2026), doi: 10.3390/computers15030189.

[2] P. Devaraj, S. A. Chaman Basha, N. N. Panarkuzhiyil Santhosh, and N. Panda, "A post-quantum secure architecture for 6G-enabled smart hospitals: A multi-layered cryptographic framework," *Future Internet*, vol. 18, no. 3, Art. no. 165 (2026), doi: 10.3390/fi18030165.

[3] H. Bourekouche, S. Belkacem, and N. Messaoudi, "Design and analysis of a pseudo random number generator based on the logistic-sine system and a nonlinear feedback shift register: Application to image encryption," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 7, pp. 2645–2670 (2025), doi: 10.47974/JDMSC-1847.

[4] D. Marbouh, M. C. E. Simsekler, K. Salah, R. Jayaraman, and S. Ellahham, "A blockchain-based regulatory framework for mHealth," *Data*, vol. 7, no. 12, Art. no. 177 (2022), doi: 10.3390/data7120177.

[5] S. Barbaria, A. Jemai, H. İ. Ceylan, R. I. Muntean, I. Dergaa, and H. Boussi Rahmouni, "Advancing compliance with HIPAA and GDPR in healthcare: A blockchain-based strategy for secure data exchange in clinical research involving private health information," *Healthcare*, vol. 13, no. 20, Art. no. 2594 (2025), doi: 10.3390/healthcare13202594.

[6] K. N. Kala and K. Vidyakala, "Bibliometric analysis of telematics applications in the automotive insurance sector," *J. Stat. Manag. Syst.*, vol. 29, no. 1, pp. 69–76 (2025), doi: 10.47974/JSMS-1488.

[7] H. Yan, Z. Wang, L. Lin, J. Sun, and S. Liu, "A Kyber-based lightweight cloud-assisted authentication scheme for medical IoT," *Sensors*, vol. 26, no. 7, Art. no. 2021 (2026), doi: 10.3390/s26072021.

[8] J. Choi and J. Lee, "Secure and scalable Internet of Things model using post-quantum MACsec," *Appl. Sci.*, vol. 14, no. 10, Art. no. 4215 (2024), doi: 10.3390/app14104215.

[9] Y. Wen, Y. Su, and W. Li, "Post-quantum secure multi-factor authentication protocol for multi-server architecture," *Entropy*, vol. 27, no. 7, Art. no. 765 (2025), doi: 10.3390/e27070765.

[10] M. Almutairi and F. T. Sheldon, "Resilience of post-quantum cryptography in lightweight IoT protocols: A systematic review," *Eng*, vol. 6, no. 12, Art. no. 346 (2025), doi: 10.3390/eng6120346.

[11] R. Campbell, "Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks," *Computers*, vol. 15, no. 1, Art. no. 9 (2026), doi: 10.3390/computers15010009.

[12] S.-Y. Chang and Q. Khan, "Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions," *Cryptography*, vol. 10, no. 1, Art. no. 12 (2026), doi: 10.3390/cryptography10010012.

[13] F. Albalwy, "Zero-knowledge-based policy enforcement for privacy-preserving cross-institutional health data sharing on blockchain," *Systems*, vol. 14, no. 4, Art. no. 385 (2026), doi: 10.3390/systems14040385.

[14] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, "Secure data transmission of electronic health records using blockchain technology," *Electronics*, vol. 12, no. 4, Art. no. 1015 (2023), doi: 10.3390/electronics12041015.

[15] S. Zhang and M. M. Singh, "Privacy and security in health big data: A NIST-guided systematic review of technologies, challenges, and future directions," *Information*, vol. 17, no. 2, Art. no. 148 (2026), doi: 10.3390/info17020148.

Received March, 2026