

Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures

Harish P. Bhabad ^{1,✉}, Anand Singh Rajawat ²

1. Computer Science and Engineering, Sandip University, Nashik, IND

2. Computer Science and Engineering, School of Computer Sciences and Engineering, Sandip University, Nashik, IND

Received: January 25, 2026 | Review began: February 01, 2026 | Review ended: April 13, 2026 | Published: May 22, 2026

© Copyright 2026

This is an open access article distributed under the terms of the Creative Commons Attribution License CC-BY 4.0., which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

Electronic health records (EHRs) security is becoming increasingly crucial as healthcare organizations embrace blockchain technology for decentralized and immutable data management. However, the advent of quantum computing poses a severe danger to the encryption techniques now used to safeguard these systems. In order to protect EHRs against future quantum assaults, this article proposes a blockchain-based security system that combines hybrid encryption with anti-quantum signatures. Specifically, we offer a hybrid signature method that combines the Elliptic Curve Digital Signature Algorithm and the post-quantum Dilithium algorithm to guarantee efficiency and quantum resistance. To further improve security by stopping bad actors from altering transactions, quantum blind signatures are also included. The proposed architecture presents a robust solution for EHR management, poised to thrive in a post-quantum future since it is made to be scalable, safe, and effective. Performance evaluations demonstrate the system's feasibility and highlight how resistant it is to quantum assaults while preserving the integrity and security of private medical data.

Categories: Quantum Algorithms, Blockchain and Cryptocurrency, Cryptographic Algorithms

Keywords: anti-quantum signatures, quantum blind signatures, ehr, ecdsa, blockchain technology

Introduction

Electronic health records (EHRs) require robust security and privacy measures to protect sensitive patient information. This article proposes a novel blockchain-based security framework for EHRs, integrating hybrid encryption and anti-quantum signatures. For sensitive patient data to be shielded against loss, alteration, and unwanted access, EHR security is essential. Strong security measures must be put in place as healthcare organizations move from paper-based records to digital platforms, increasing the danger of data breaches and cyberattacks. EHRs hold private and sensitive health data that, if stolen, can result in medical fraud, identity theft, and serious privacy violations [1]. Maintaining the privacy of this information is crucial as its unapproved release might have serious repercussions for patients and medical professionals alike. Furthermore, the correct operation of healthcare systems depends on the integrity of EHRs. To make well-informed judgments about diagnosis and treatment plans, healthcare professionals depend on current, reliable patient data [2]. This data might result in harmful mistakes that could endanger patient care and possibly even save lives if it is changed or distorted. Thus, preserving the quality and safety of healthcare delivery depends critically on safeguarding the integrity of EHRs. Furthermore, as medical personnel depend on immediate access to patient records for routine consultations, emergency care, and ongoing treatments, EHR systems must be always accessible. Treatment delays, patient health risks, and the effectiveness of the healthcare system can result from any interruption in the availability of these records, whether due to technological difficulties, system malfunctions, or cyberattacks [3]. Therefore, maintaining the availability of EHRs is equally as crucial as protecting their integrity and confidentiality. Regulations that enforce strict

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

guidelines for the processing, sharing, and retaining of health data, emphasize the need for strong security in EHRs. Legal and financial consequences may arise from breaking these rules, underscoring the significance of protecting EHRs from possible dangers. Finally, patient confidence in healthcare systems is closely related to the security of EHRs. Patients need to have faith that their private health data are secure and managed appropriately. The efficacy of healthcare is eventually impacted by breaches because they undermine confidence and make patients reluctant to divulge critical medical information. Thus, EHR security is not just a technological issue, it is also essential to upholding confidence and guaranteeing the prosperity of contemporary healthcare systems. Blockchain technology has become a potent remedy for the problems with immutability, security, and transparency that EHR systems confront [4]. By offering a decentralized, tamper-resistant ledger that ensures sensitive patient data are secure and verifiable at every point of its existence, blockchain may significantly enhance the storage, sharing, and accessibility of healthcare data [5]. On the other hand, blockchain creates an unchangeable chain of records by securely encrypting each transaction (or record update) and connecting it to the one before it. Once a health record is added to the blockchain, it cannot be altered or deleted without network consensus, protecting the patient's medical history. Blockchain also makes data exchange transparent and safe [6]. Patients frequently get care from several providers in a healthcare setting, and it is necessary for different institutions to communicate their medical data. Because blockchain technology is decentralized, authorized parties may share EHRs in a transparent and safe manner without the need for a central middleman. By limiting access to their data to trustworthy healthcare practitioners and making sure that their records are shared only with their permission, patients may keep control over their data. Accountability and auditability are two more essential characteristics that blockchain offers [7]. A timestamp and digital signature are attached to each transaction on the blockchain, allowing one to track who accessed or changed a certain record and when. Because any inconsistencies or unlawful activity may be promptly detected, this improves accountability within the healthcare system. Additionally, blockchain can facilitate a thorough audit trail, guaranteeing adherence to laws like General Data Protection Regulation and Health Insurance Portability and Accountability Act. Additionally, there is an opportunity to automate some healthcare processes by combining blockchain technology with smart contracts [8]. Smart contracts may streamline processes and lessen administrative expenses by enabling things like automatically updating medical records when specific criteria are satisfied or confirming patient permission for data sharing. Blockchain also promotes patient empowerment. Because it makes it possible for personal health information to be managed in a more transparent and safe manner, this empowerment promotes confidence and cooperation between patients and healthcare professionals. To sum up, blockchain presents a workable solution to enhance the security, privacy, and interoperability of EHR systems [9]. It is the perfect solution to solve many of the issues that traditional EHR systems encounter because of its capacity to guarantee data integrity, facilitate safe data exchange, provide auditability, and empower patients. Blockchain's incorporation into healthcare might result in more effective, safe, and patient-centered health record management as it develops.

The advent of quantum computing poses a significant danger to existing cryptography methods, which form the basis of data security in several fields, including the safeguarding of EHRs [10-12]. However, these cryptographic techniques might be attacked since quantum computers could solve these issues much quicker than conventional computers. Shor's method can efficiently factor large numbers and compute discrete logarithms in polynomial time, as opposed to the exponential time required by traditional algorithms, and quantum techniques in particular. Popular encryption methods like Rivest-Shamir-Adleman algorithm (RSA) and elliptic curve cryptography (ECC), which are meant to protect sensitive data, are at risk from this capability due to the intricacy of these problems. Privacy, integrity, and trust across digital systems, including healthcare, might be jeopardized if quantum computers have enough capacity to decode data that is presently regarded as safe. This issue is especially relevant to EHRs. To maintain security and integrity during storage and transmission, healthcare data including medical histories and personal health information are frequently encrypted using RSA or ECC. These encryption techniques could become outdated due to quantum computing, leaving private medical information vulnerable to manipulation or illegal access. The necessity for quantum-resistant cryptography is further increased by the fact that health data storage is a long-term process, meaning that encrypted data may need to be safe for decades. Quantum computing has the potential to compromise digital signature systems in addition to cracking conventional encryption [13-15]. Quantum computers may be able to crack the cryptographic methods that digital signatures rely on to authenticate transactions and confirm data integrity. This would make it possible for bad actors to

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

fake signatures, jeopardizing the security of vital systems that depend on integrity and authenticity, such as electronic health data. Additionally, blockchain systems, which depend on cryptographic methods to guarantee the immutability of records, are under risk from quantum computing. Despite the intrinsic security offered by blockchain's decentralized structure, quantum assaults can nevertheless affect the cryptographic underpinnings of the system. Post-quantum cryptography, or new cryptographic algorithms made to withstand quantum assaults, is being intensively studied by the cryptographic community in response to this new danger. These include lattice-based encryption, hash-based signatures, and other quantum-resistant techniques that might replace long-standing cryptographic norms [16-17]. Sectors like healthcare must begin preparing for and transitioning to quantum-safe encryption solutions in order to protect sensitive data in a post-quantum future.

Materials And Methods

Literature review

Blockchain technology, initially developed for bitcoin, has shown significant potential in healthcare, especially for safeguarding EHRs, enhancing privacy, and promoting interoperability. Its decentralized and immutable nature addresses major issues like patient privacy, data security, and seamless data exchange. Demonstrated blockchain's ability to secure EHRs by ensuring decentralized control and access only to authorized individuals, despite challenges like interoperability and scalability [18-19]. They proposed a blockchain-based health data framework granting patients control over their medical records, improving data integrity, and reducing breaches [1]. Similarly, the explored blockchain's potential to enhance patient privacy and security by minimizing third-party dependencies, though integrating it with current healthcare systems remains challenging [3]. Blockchain's role in secure medical data sharing was investigated by Haleem et al. [6], who highlighted the use of cryptographic keys and smart contracts to enable secure and automated data sharing. In supply chain management, it was demonstrated how blockchain could trace pharmaceutical products from production to distribution, ensuring authenticity and reducing counterfeit drugs. It emphasized blockchain's ability to verify the quality and origin of medical supplies, improving patient safety [2]. Despite these benefits, blockchain faces hurdles like scalability, regulatory compliance, and integration with legacy systems. It noted issues like high processing costs and the need for supportive regulatory frameworks [7], while suggested off-chain storage and sharding to address scalability concerns [8]. Future research by Li et al. and Zu et al. [20-21] emphasized scalable solutions and integrating blockchain with Artificial Intelligence and Internet of Things to create secure, efficient healthcare ecosystems. In summary, blockchain has the potential to revolutionize healthcare by improving data security, privacy, and transparency [22]. Overcoming challenges like scalability and regulatory barriers is crucial for its widespread adoption and impact.

Cryptographic techniques for EHR security

The classification of cryptographic methods commonly used in EHR security is illustrated in Figure 7, highlighting symmetric, asymmetric, and post-quantum cryptographic techniques. Security is crucial for protecting sensitive EHRs, and robust cryptographic techniques are essential for safeguarding patient privacy and ensuring data accuracy and accessibility. This section explores various cryptographic methods used to secure EHR systems, including both traditional and advanced strategies. Symmetric encryption, particularly advanced encryption standard (AES), is commonly used in healthcare for its strong security and efficiency. However, a key management challenge arises, as the encryption key must be kept secure. Asymmetric encryption methods like RSA and ElGamal address this by eliminating the need for key distribution, although they can be computationally expensive, especially in large healthcare datasets. Digital signatures, such as Elliptic Curve Digital Signature Algorithm (ECDSA), are used to confirm data authenticity and integrity in EHRs. They ensure that only authorized professionals can modify data and provide a traceable record of all interactions with patient records. Hashing techniques like secure hash algorithm (SHA)-256 also ensure data integrity by producing a unique value for each record, making it easy to detect unauthorized changes. Homomorphic encryption enables processing of encrypted data without decryption, preserving confidentiality. Fully Homomorphic Encryption allows healthcare professionals to analyze data while maintaining patient privacy, though it is computationally intensive. Quantum-resistant cryptographic methods, such as lattice-based encryption, are being researched to protect against future quantum computing threats. Blockchain technology, in combination with cryptographic techniques, offers a

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

decentralized and immutable way to protect EHRs. Blockchain ensures secure data transfer, auditability, and authentication, enhancing interoperability while maintaining patient privacy. Although blockchain-based solutions hold promise, challenges like key management, scalability, and regulatory compliance remain. Ongoing research in cryptography, particularly regarding quantum computing, will be crucial for the future of healthcare data security.

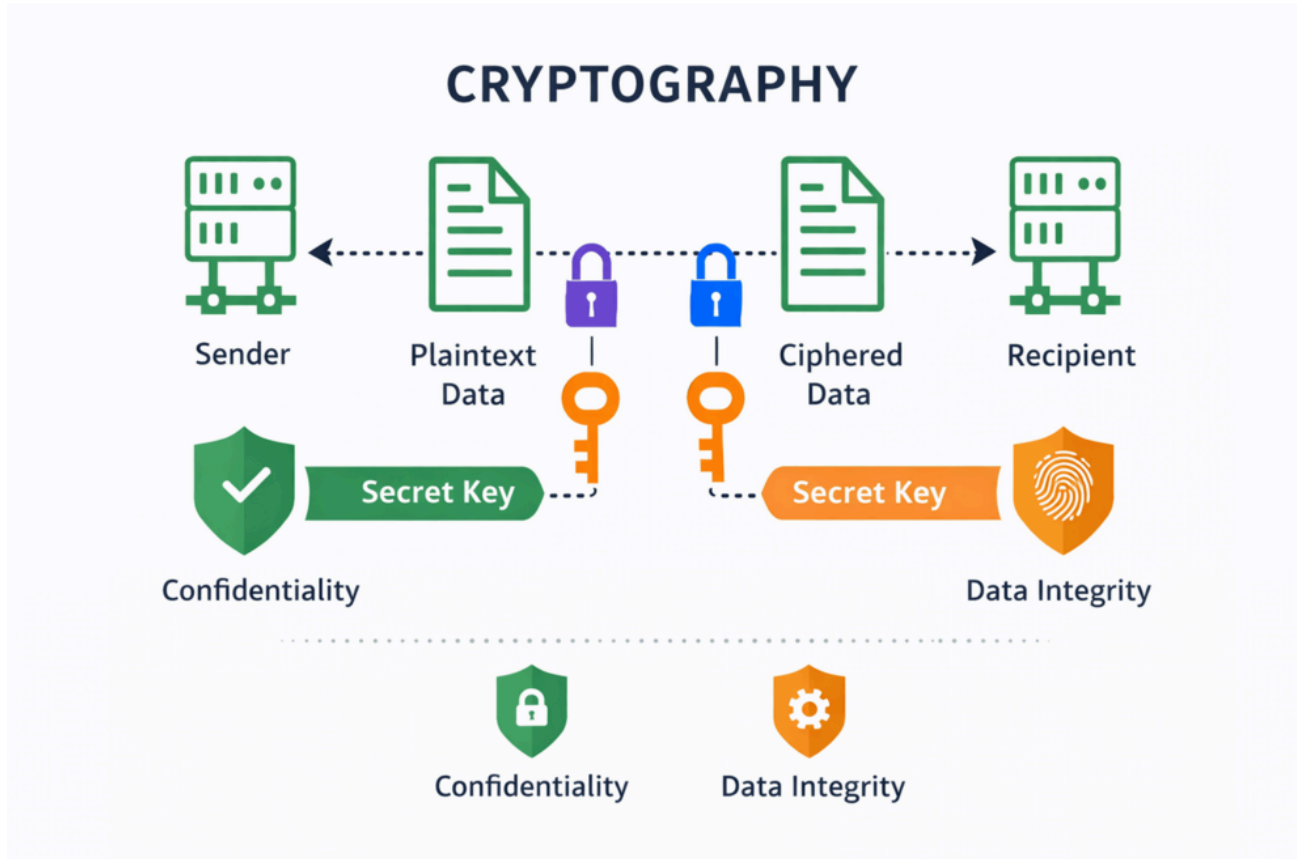


FIGURE 1: Cryptography and its types.

Anti-quantum cryptography

The rise of quantum computing poses a significant threat to the security of sensitive data, including EHRs, which are currently protected using traditional cryptographic methods like ECC and RSA. As quantum computers advance, these techniques may no longer provide adequate security. Therefore, exploring anti-quantum cryptography solutions is crucial for safeguarding patient data in the healthcare industry. Post-quantum cryptography focuses on developing encryption methods, digital signatures, and key exchange protocols that are resistant to quantum attacks. Traditional cryptography relies on mathematical problems that quantum computers could potentially solve, jeopardizing the confidentiality of sensitive information. In response, post-quantum cryptography uses problems that remain difficult for quantum computers to solve, offering a promising solution to protect health data. Quantum-resistant encryption ensures the security of EHRs during transfer and storage, while post-quantum digital signatures preserve the integrity of the data against quantum decryption methods. Blockchain-based EHR systems can further enhance security by ensuring data immutability. However, challenges like scalability, efficiency, and compatibility with legacy healthcare systems remain. Despite these issues, ongoing research in post-quantum cryptography offers a path to ensure the long-term security of healthcare data and protect patient privacy against emerging quantum threats.

How to cite this article:

Proposed approach

Blockchain-Based Hybrid Encryption Architecture

The overall blockchain-based hybrid encryption framework proposed in this study is presented in Figure 2, demonstrating the integration of blockchain, hybrid encryption, and quantum-resistant signatures. To make sure that EHRs are secure both today and in the future, this architecture combines blockchain technology with cutting-edge cryptographic approaches like hybrid encryption and quantum-resistant signature schemes. A number of essential elements make up the suggested architecture, which when combined offer a strong security solution for EHRs. These elements include anti-quantum signature systems for authenticity and defense against quantum assaults, symmetric and asymmetric hybrid encryption for data secrecy, and blockchain for data integrity. The core of the proposed concept is blockchain technology, which provides a decentralized, transparent, and immutable ledger system. Blockchain guarantees tamper-proof recording of all EHR modifications. A chain of records that cannot be changed covertly is created by storing each EHR record as a block that is cryptographically connected to the one before it. Since a block cannot be removed or altered once it is uploaded to the blockchain, patient data are kept safe against manipulation and unwanted changes. To ensure that everyone involved in patient care has access to the same reliable data, authorized users can utilize the blockchain to confirm the accuracy of EHR data. Blockchain guarantees transparency and data integrity, but it does not automatically safeguard EHR confidentiality.

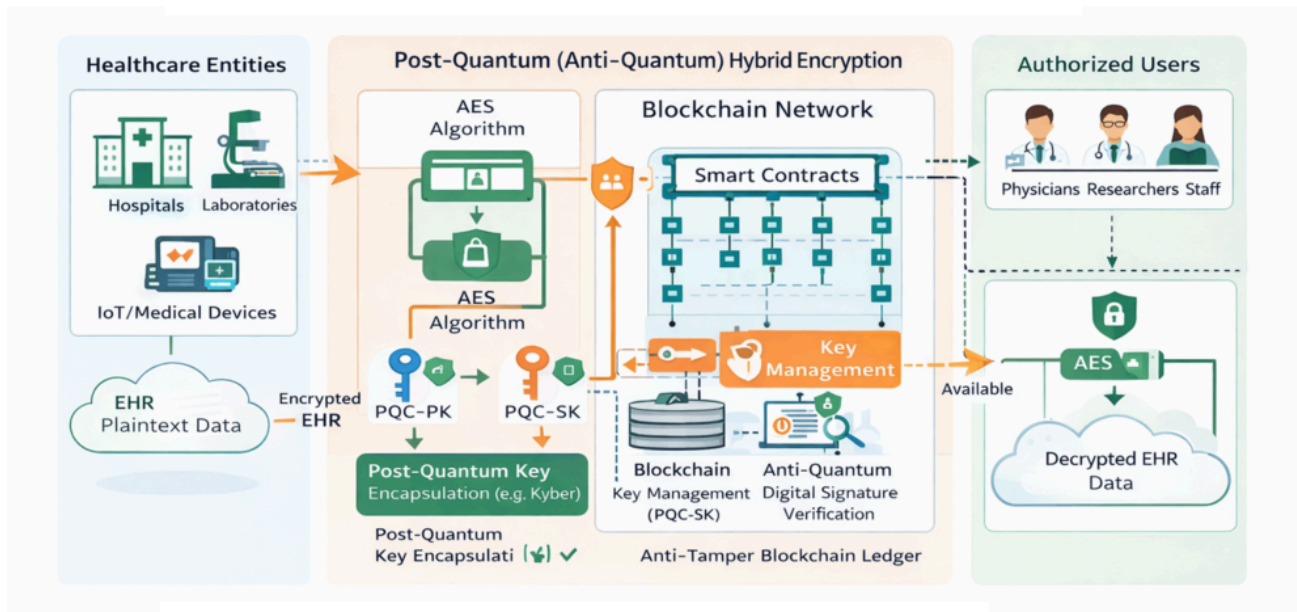


FIGURE 2: Blockchain-based hybrid encryption.

AES, advanced encryption standard; EHR, electronic health records.

The combination of post-quantum and standard signatures protects the system against both classical and quantum attacks. The suggested architecture incorporates quantum-resistant key exchange protocols to safely transfer encryption keys between healthcare organizations and providers. These methods ensure that private data are protected during transmission, even in the face of possible quantum threats. The architecture makes sure that EHR data are secure while it is being sent between healthcare organizations, providers, and patients by using quantum-resistant key exchange techniques. The hybrid encryption architecture built on the blockchain is intended to work with the current healthcare system. Healthcare practitioners may preserve private and secure patient data while taking advantage of blockchain's transparency and immutability thanks to its easy integration with EHR systems. diverse healthcare providers can safely exchange patient data across platforms because of the system's ability to communicate with diverse healthcare systems

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

via standardized application programming interfaces. Large volumes of patient data may be accommodated by the design, guaranteeing that security will not be compromised without performance issues as the healthcare system expands. The suggested architecture's resilience to potential threats from quantum computing is one of its primary characteristics. Existing cryptography methods will become more susceptible as quantum computers gain power. EHR security is maintained as quantum technology develops thanks to the architecture's integration of hybrid encryption techniques and post-quantum cryptography. By using quantum-resistant encryption techniques, the healthcare system can defend against quantum attacks and protect sensitive health data over the long term. A complete solution for protecting EHR from both present security issues and new quantum threats is provided by the suggested blockchain-based hybrid encryption architecture. By combining the immutability of blockchain technology with secure key exchange protocols, hybrid encryption, and digital signatures that are impervious to quantum assaults, this architecture ensures the confidentiality, authenticity, and security of EHRs. Because the suggested method is future-proof, healthcare organizations will be able to safeguard patient data even as the threat posed by quantum computing increases.

Anti-Quantum Signature Mechanisms

The development of quantum computing poses a severe challenge to the traditional cryptographic systems that ensure the security of sensitive data, such as EHRs. RSA and the ECDSA are two instances of traditional cryptographic techniques that can be successfully cracked by quantum algorithms, particularly Shor's method. To guarantee the ongoing security of EHRs, this vulnerability emphasizes the need for the development of anti-quantum encryption, particularly post-quantum digital signatures. Utilizing the complexity of lattice problems that are believed to be immune to quantum algorithms lattice-based cryptography is one of the most promising techniques for post-quantum digital signatures. It is a top option for protecting EHRs due to its great efficiency and robust security. Even if problems with processing efficiency and large key sizes still exist, the integration of these state-of-the-art cryptographic algorithms into blockchain-based EHR systems will provide a robust, future-proof security solution.

Integration of Quantum Blind Signatures

Ensuring the security and integrity of EHRs in the nascent era of quantum computing requires the integration of Quantum Blind Signatures (QBS) into blockchain-based systems. The working principle of the QBS mechanism is depicted in Figure 3, showing how data privacy is preserved during the signing process. Adopting quantum-resistant cryptography is essential as conventional encryption methods are exposed to quantum assaults, particularly for sensitive data like medical records. Blind signatures provide a special way to guarantee that a communication or document may be signed by one party without disclosing its contents to the signer. They have been extensively utilized in privacy-preserving applications. In the healthcare industry, where confidentiality and privacy are crucial, this trait is very significant. By using quantum-resistant techniques, QBS expand on the idea of blind signatures. Unlike traditional blind signatures that rely on cryptographic techniques like elliptic curve encryption or RSA, which are both vulnerable to such attacks, QBS use advanced post-quantum cryptography techniques that are immune to quantum algorithms like Shor's algorithm. These algorithms often rely on lattice-, hash-, or code-based encryption to provide security even when a quantum computer is present. The use of QBS into blockchain improves security and privacy. A strong foundation for storing and validating EHRs is offered by blockchain's intrinsic decentralization, transparency, and immutability features. Blockchain technology, when used in conjunction with QBS, guarantees that patient anonymity may be maintained while healthcare data are safely signed and kept. In order to ensure that the signer cannot see the contents of the data, the procedure starts with the patient or healthcare practitioner blinding the health record. After being blindfolded, the information is given to a reliable individual or organization, such a healthcare professional, to be signed. The blinded record is subjected to the signature, which is produced using a quantum-resistant cryptographic procedure. Following the signing procedure, the original health data's signature is visible when the record is unblinded. This maintains the secrecy of the patient's sensitive information while guaranteeing that the signed data can still be verified. There are a number of significant benefits of using QBS in blockchain-based EHR systems. First, it ensures patient privacy because the signer never sees the information in the medical record. Second, by using quantum-resistant techniques, the security of the signed papers is shielded from any threats posed by quantum computing. Blockchain technology's immutability further improves the security of these documents by forbidding unauthorized alterations once they are recorded.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

Furthermore, without sacrificing security, the decentralized architecture of blockchain enables transparent record verification by a number of stakeholders, including patients, healthcare providers, and regulatory agencies. Nevertheless, there are inherent difficulties in incorporating QBS into blockchain-based EHR systems. The intricacy of putting quantum-resistant algorithms into practice might result in extra computing overhead and affect system performance. As quantum computing advances, the employment of quantum-resistant encryption algorithms, such as QBS, will be essential for maintaining the privacy and security of electronic health data. Figure 3 illustrates the standard Digital Signature generation and verification algorithm process, adapted from classical public-key cryptography models, Menezes et al. [23].

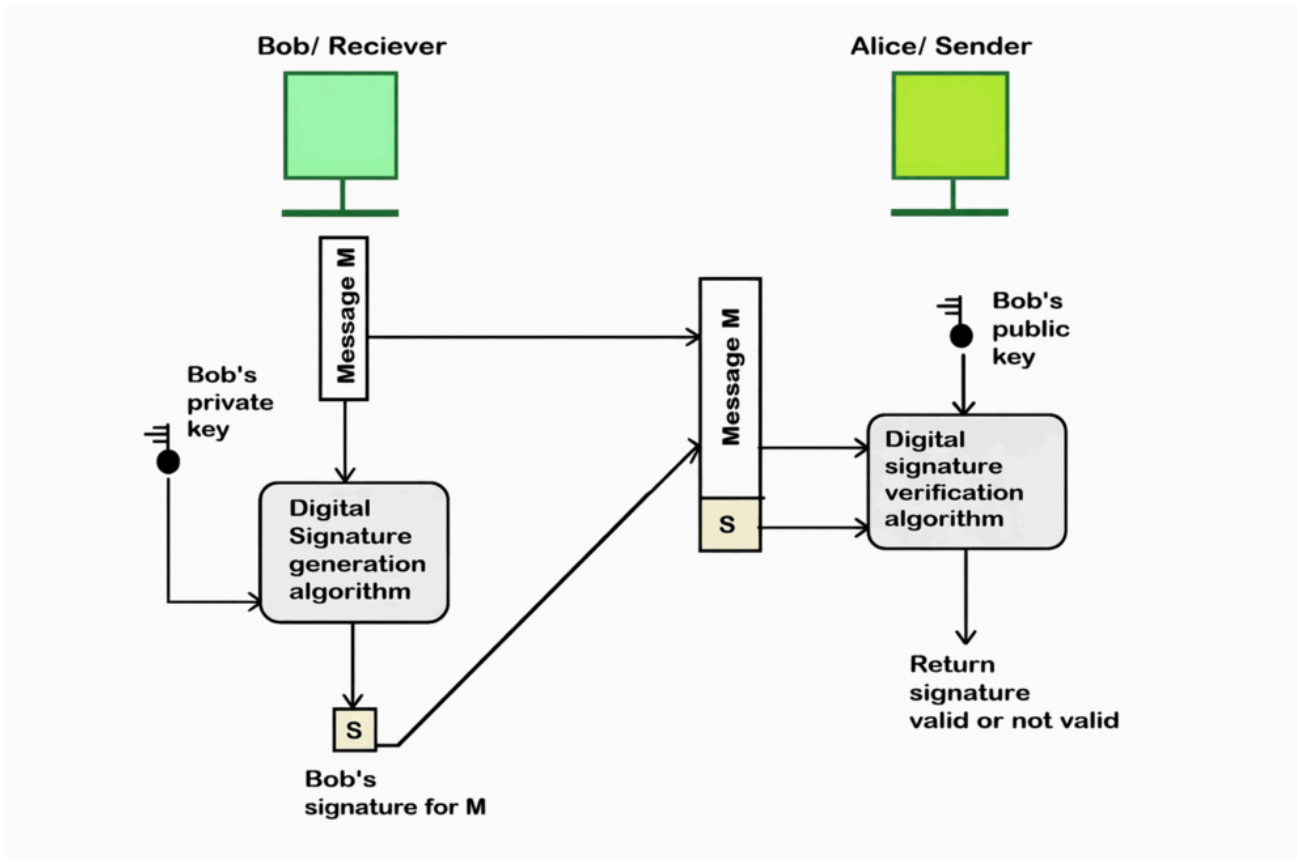


FIGURE 3: Quantum blind signature.

Hybrid signature scheme combining ECDSA and Dilithium

The rapid advancement of quantum computing poses a serious threat to conventional public-key cryptographic schemes that underpin blockchain-based EHR systems. Classical digital signature algorithms such as ECDSA rely on the computational hardness of the Elliptic Curve Discrete Logarithm Problem, which can be efficiently solved by quantum algorithms such as Shor's algorithm. To address this emerging vulnerability while preserving backward compatibility with existing blockchain infrastructures, this work proposes a hybrid digital signature scheme that integrates ECDSA with the post-quantum lattice-based Dilithium signature algorithm.

The structure of the hybrid digital signature scheme combining ECDSA and Dilithium is illustrated in Figure 4, ensuring resistance against both classical and quantum attacks. In this scheme, each blockchain transaction or EHR record is signed using two independent cryptographic signatures, ensuring long-term data authenticity and integrity even in the presence of large-scale quantum computers.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

During verification, the recipient validates both signatures independently. The ECDSA signature is verified using classical elliptic curve techniques, while the Dilithium signature is verified using lattice-based verification procedures. A transaction is considered valid only if both verifications succeed, thereby ensuring resistance against both classical and quantum attacks. Hybrid Signature Scheme is adapted from Linke B, using the ECSDA effectively [24].

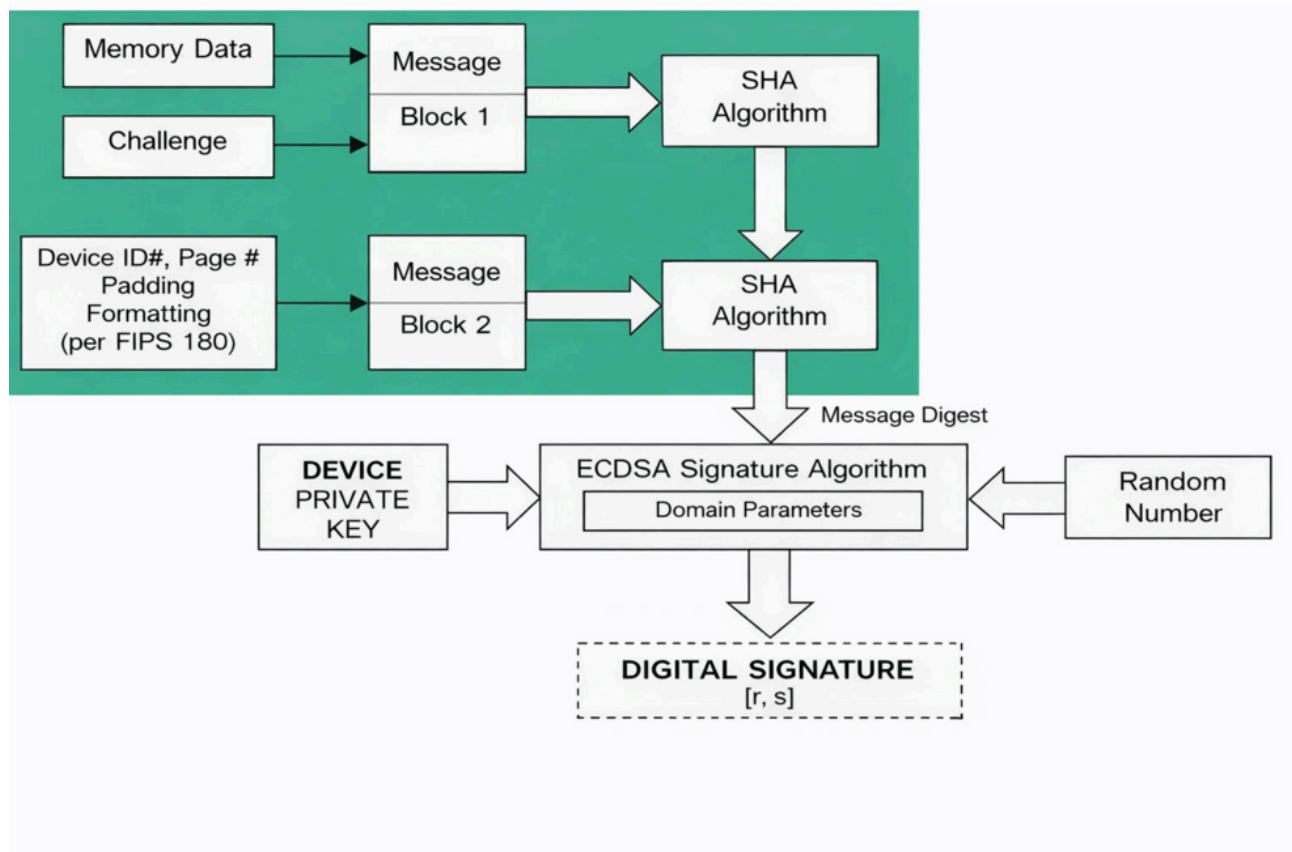


FIGURE 4: Hybrid signature scheme.

ECDSA, Elliptic Curve Digital Signature Algorithm; SHA, secure hash algorithm.

Digital signature algorithm

The Digital Signature Algorithm (DSA), standardized by the National Institute of Standards and Technology as part of the Digital Signature Standard (DSS), is based on the hardness of the Discrete Logarithm Problem (DLP) in finite fields.

Key Generation for DSA

In order to generate keys for DSA, a public-private key pair must be created:

1. **Select a prime number p :** To construct the finite field utilized in DSA, select a large prime integer p .
2. **Choose a generator g :** Choose a generator g is chosen from the multiplicative group modulo p .
3. **Choose a private key x :** Choose the private key to be a secret integer x . The private key has to be kept private.
4. **Compute the public key y :** The formula for the public key y is computed using the formula $y = g^x \bmod p$. The public key y is made accessible for the purpose of verifying signatures.

While the public key y is shared with others to validate signatures, the private key x is kept confidential.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

Signature Generation for DSA

DSA generates a unique, non-forgeable signature (r, s) for a message m using a private key x and a secure hash function.

To generate a signature for a message using DSA:

1. Message Hashing: To create a message digest $H(m)$, the message m is first hashed using a secure hash algorithm (such as SHA-1 or SHA-256).
2. Generate random value k : Select a random integer k from the set $\{1, 2, \dots, q-1\}$. The value k must be kept secret and unique for each signature.
3. Compute the signature components:

r Component: $r = (g^k \bmod p) \bmod q$, where p and q are prime parameters and g is a generator.

s Component: $s = k^{-1} \cdot (H(m) + x \cdot r) \bmod q$, where x is the signer's private key, and k^{-1} is the modular inverse of k modulo q .

4. Final Signature: The digital signature consists of the pair (r, s) which is sent along with the message.

The recipient can then use the public key y to verify the authenticity of the signature.

The DSA, standardized by NIST as part of the DSS, is based on the hardness of the DLP in finite fields.

Elliptic curve digital signature algorithm

The ECDSA is a variant of DSA that is based on elliptic curves. Modern encryption, particularly blockchain systems like Ethereum and Bitcoin, makes extensive use of ECDSA. It is more effective for usage in limited contexts, including mobile devices and blockchain networks, because it offers the same functionality as DSA but with smaller key sizes and improved security.

Key Generation for ECDSA

The key generation process for ECDSA is similar to DSA, but it is based on elliptic curve arithmetic:

1. Choose an elliptic curve: Choose a curve that is elliptic. Certain security requirements, such as a big prime order group, should be satisfied by the curve.
2. Select a private key x : Select the private key, which is kept secret, to be a secret integer x .
3. Compute the public key: Determine the public key $Q = x \cdot G$, where x is the private key and G is a base point on the elliptic curve.

While the public key Q is used to validate the signatures, the private key x is kept secret.

Signature Generation for ECDSA

To generate a signature for a message using ECDSA: creating a pair of integers (r, s) that represent a digital signature for a given message using a private key and a random, ephemeral nonce k .

1. Message Hashing: Hash the message m using a cryptographic hash function (e.g., SHA-256 or Keccak256) to produce a hash value $e = H(m)$.
2. Generate random value k : Choose a random number k from the range $(1, 2, \dots, n - 1)$, where n is the elliptic curve's base point. This value must be unique for each signature and kept secret.
3. Compute Point R and Component r : Compute the elliptic curve point

$$R = k \times G = (x_1, y_1)$$

$$\text{Set } r = x_1 \bmod n$$

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

If $r = 0$, you must choose a new random k and restart.

4. Compute the signature components:

$$s = k^{-1}(e + x \cdot r) \bmod n$$

If $s = 0$, you must choose a new random k and restart.

5. Signature: The pair (r, s) is the digital signature that is transmitted with the message.

Dilithium: post-quantum signature scheme

Dilithium is a NIST-standardized, lattice-based digital signature scheme whose security is based on the hardness of the Module Learning with Errors and Short Integer Solution problems. Its structured lattice design ensures efficiency while maintaining strong quantum resistance. The algorithm's three main steps are key generation, signature generation, and signature verification.

Key Generation

The key generation process produces a public-private key pair:

1. Parameter Selection: Choose parameters q, k, l, η, γ based on the desired security level.

according to the required security level, where q denotes the modulus, k and l define the matrix dimensions, and η control the bounds of the sampled secret values and γ define bound for rejection sampling.

2. Generate Matrix A: Create a uniformly random matrix A of size $k * l$ over $\mathbb{Z}_q$.

This matrix defines the public lattice.

$$A \in \mathbb{Z}_q^{k \times l}$$

3. Sample Secret Vectors: Sample two secret vectors $s_1 \in S_\eta^l$ and $s_2 \in S_\eta^k$ of dimensions l and k , respectively. The elements are drawn from a discrete Gaussian distribution bounded by η .

4. Compute Public Key: Compute $t = A \cdot s_1 + s_2 \bmod q$, where $\cdot$ is matrix-vector multiplication. The public key consists of A and t .

5. Output:

Public Key: (A, t)

Private Key: (s_1, s_2)

Signature Generation

The signature creation process uses the private key to sign a message:

1. Hash Message: Hash the message m into a uniform vector c of size k using a cryptographic hash function.

$$c = H(m) \in \{0, 1\}^k$$

2. Generate a Random Vector: Sample a random vector y from a bounded discrete Gaussian distribution.

$$y \leftarrow \mathcal{D}_\eta^l$$

3. Compute Intermediate Values:

$w = A \cdot y \bmod q$: Multiply the random vector y with the public matrix A .

w_1 : Extract the higher-order bits of w for efficient rejection sampling.

4. Compute Challenge: Use w_1 and the message hash $H(m)$ to compute a challenge vector cc using a cryptographic hash function.

How to cite this article:

5. Compute Signature Components:

$z = y + c \cdot s_1$: Add the scaled private key s_1 to y , weighted by the challenge c .

Perform rejection sampling to ensure z satisfies certain bounds.

6. Output Signature: The signature is $\sigma = (z, c)$

Signature Verification

The authenticity of the signature σ for the given public key and message is verified using the signature verification process:

1. Recompute Intermediate Values:

$$w' = A \cdot z - c \cdot t \bmod q$$

Extract w_1 , the higher-order bits of w' .

2. Recompute Challenge:

$$c' = H(w_1, H(m))$$

Use w_1 and the message hash $H(m)$ to recompute the challenge c' .

3. Verify Consistency:

Check if $c' = c$: If the challenges match, the signature is valid.

Ensure that z lies within the specified bounds.

4. Output:

If all conditions are satisfied, the signature is $c' = c$ accepted as valid. Otherwise, it is rejected.

A potential post-quantum signature system that blends effectiveness, portability, and strong security is called Dilithium. It guarantees resistance against present and upcoming cryptographic issues by utilizing the difficulty of lattice-based problems, which makes it the perfect option for protecting vital systems like financial systems, healthcare platforms based on blockchain, and other delicate digital infrastructures.

Results And Discussion

Experimental setup

To evaluate the effectiveness and feasibility of the proposed blockchain-based hybrid encryption framework with anti-quantum signatures, a comprehensive experimental setup was designed and implemented using Solidity language, provided by Ethereum, encapsulates JavaScript and Python. The simulation environment was configured to emulate a realistic healthcare blockchain network supporting EHR transactions under varying operational conditions.

The experimental model consists of multiple healthcare entities acting as blockchain nodes, including hospitals, diagnostic centers, and authorized healthcare providers. Each node participates in transaction generation, verification, and block validation. A permissioned blockchain architecture was assumed to reflect practical healthcare deployment scenarios, where only authenticated entities are allowed to access and update EHR data.

Python is selected for this study owing to its versatility, stability, and rich ecosystem of libraries, which facilitate efficient modeling, simulation, and analysis of complex systems. To guarantee safe data transactions inside a blockchain framework, the system integrates anti-quantum cryptographic techniques and hybrid encryption systems. The simulation environment is made to mimic how the blockchain would behave in various situations and with varying user loads, including consensus processes, transaction validation, and ledger replication. Important features, including hybrid encryption that combines post-quantum and classical algorithms, are put into practice and evaluated for how well they

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

secure EHRs. Furthermore, anti-quantum signature techniques are modeled to show how resilient they are against assaults by quantum computing, such as the combination of lattice-based Dilithium signatures with ECDSA. Critical performance indicators like throughput, latency, and scalability are assessed during the simulation to gauge the effectiveness and resilience of the system. The throughput performance of the proposed system, measured in KB/second under varying workloads, is shown in Figure 5. The simulation's outcomes validate the framework's capacity to safely manage substantial amounts of medical data while preserving respectable performance levels. By verifying the feasibility of using the suggested method in actual EHR management situations, these simulations provide increased protection against new quantum threats.

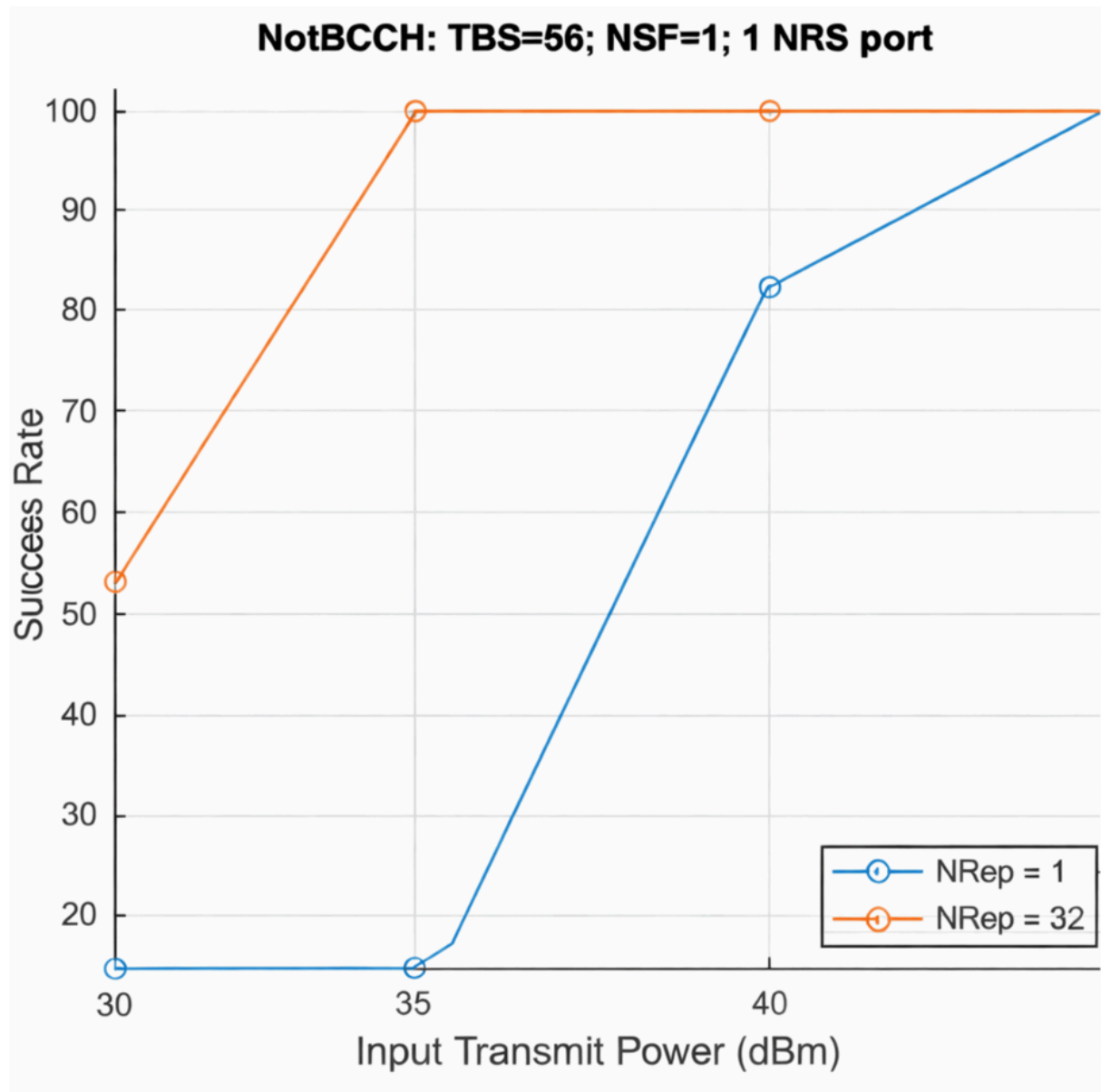


FIGURE 5: Throughput measured in KB/second.
NRF, network repository function; NSF, network security function; TBS, to be signed.

The units of data per unit time, or KB/second, are used to quantify throughput. We ran simulations based on the designated number of users during testing to evaluate the efficacy of the system. The suggested framework was used to run these simulations, and once they were finished, throughput was assessed.

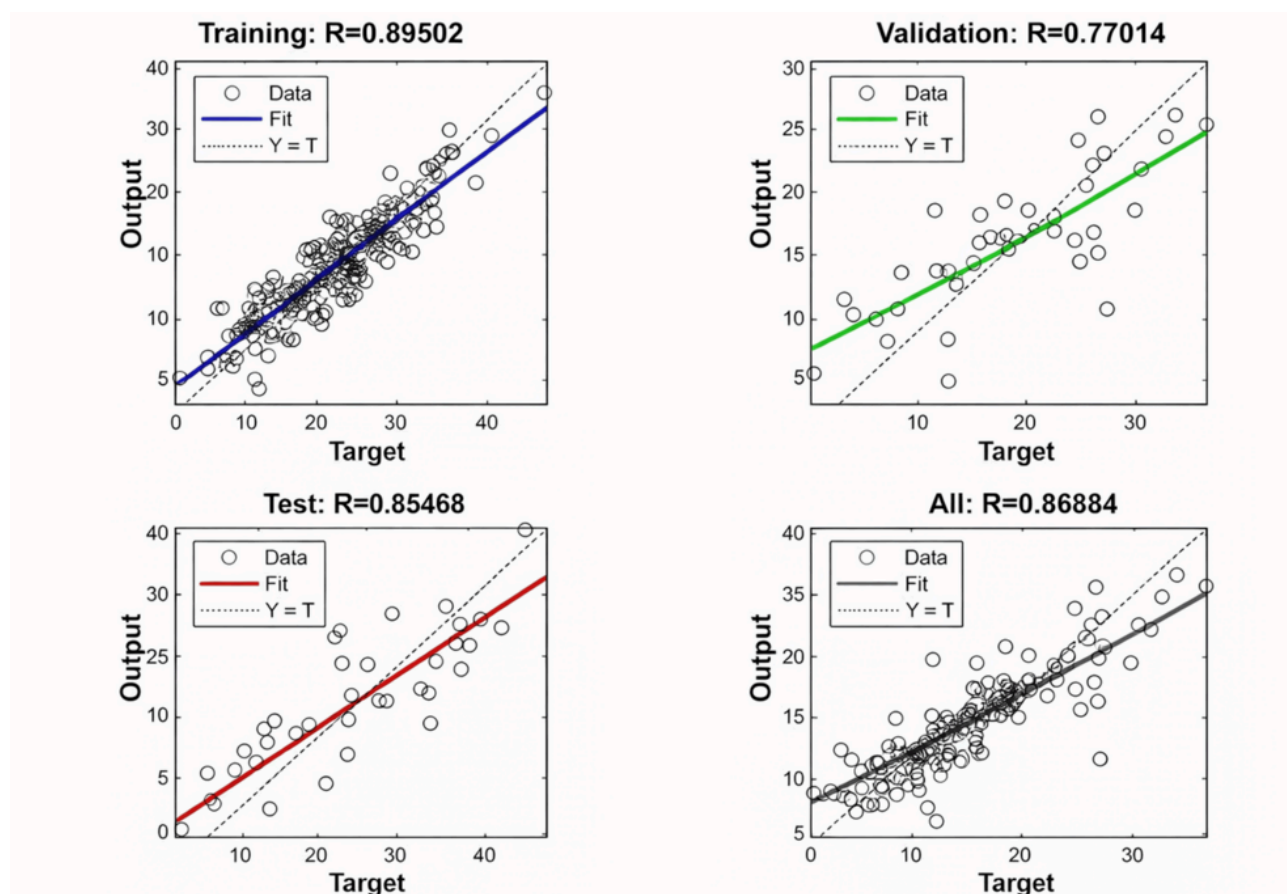


FIGURE 6: Regression analysis of waveform target.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

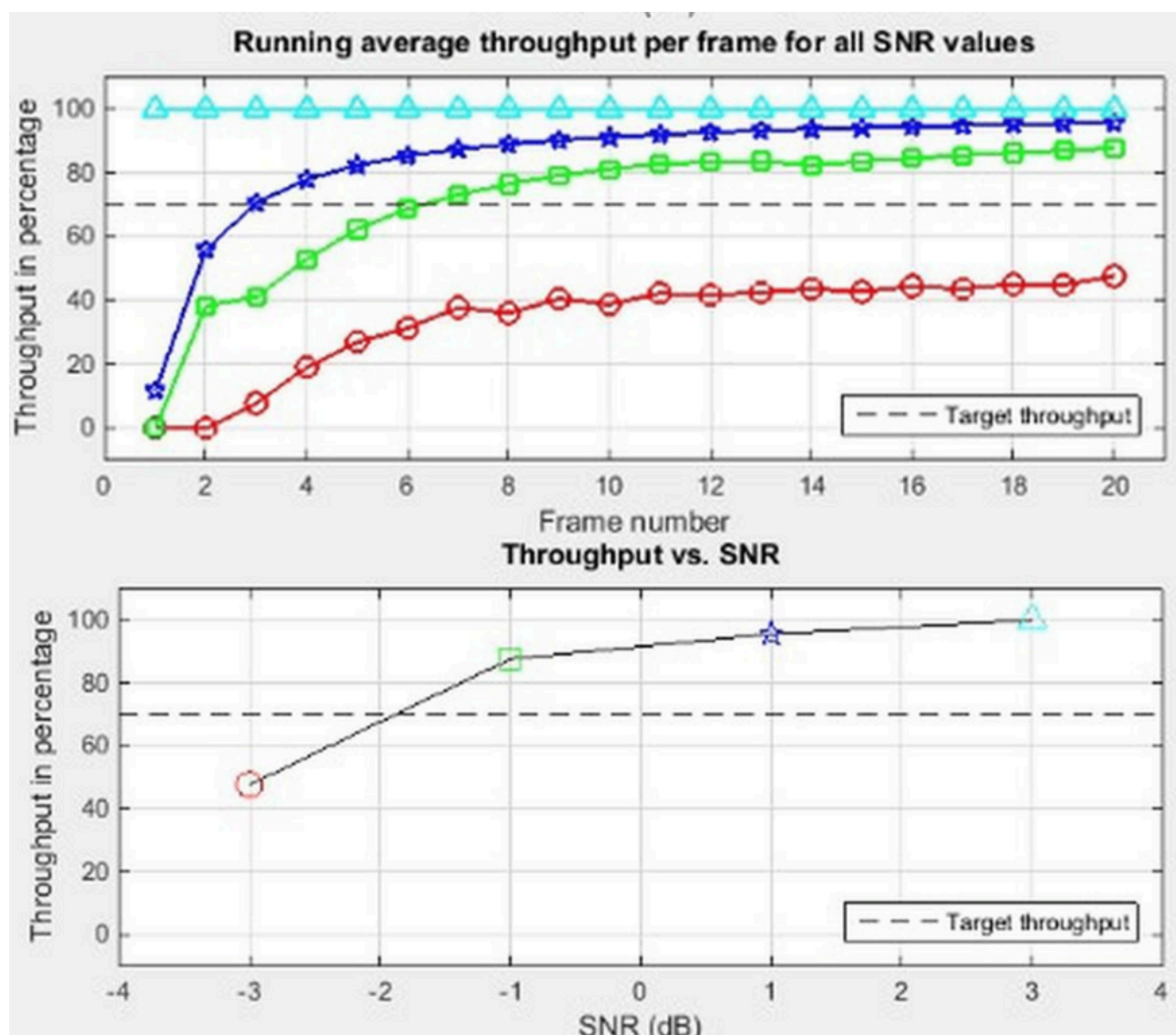


FIGURE 7: Performance analysis of transaction throughput.

SNR, signal-to-noise ratio.

The waveform characteristics observed during system operation are presented in Figure 6, validating the stability of the proposed framework. The graphic displays an effective trade-off between data processing speed and transmission time. The average delay stays within reasonable bounds as throughput rises. A detailed performance analysis of transaction throughput is provided in Figure 7, illustrating scalability under increased transaction volume. This illustrates the suggested method's scalability, showing that it can manage larger transaction volumes without seeing appreciable increases in processing time.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

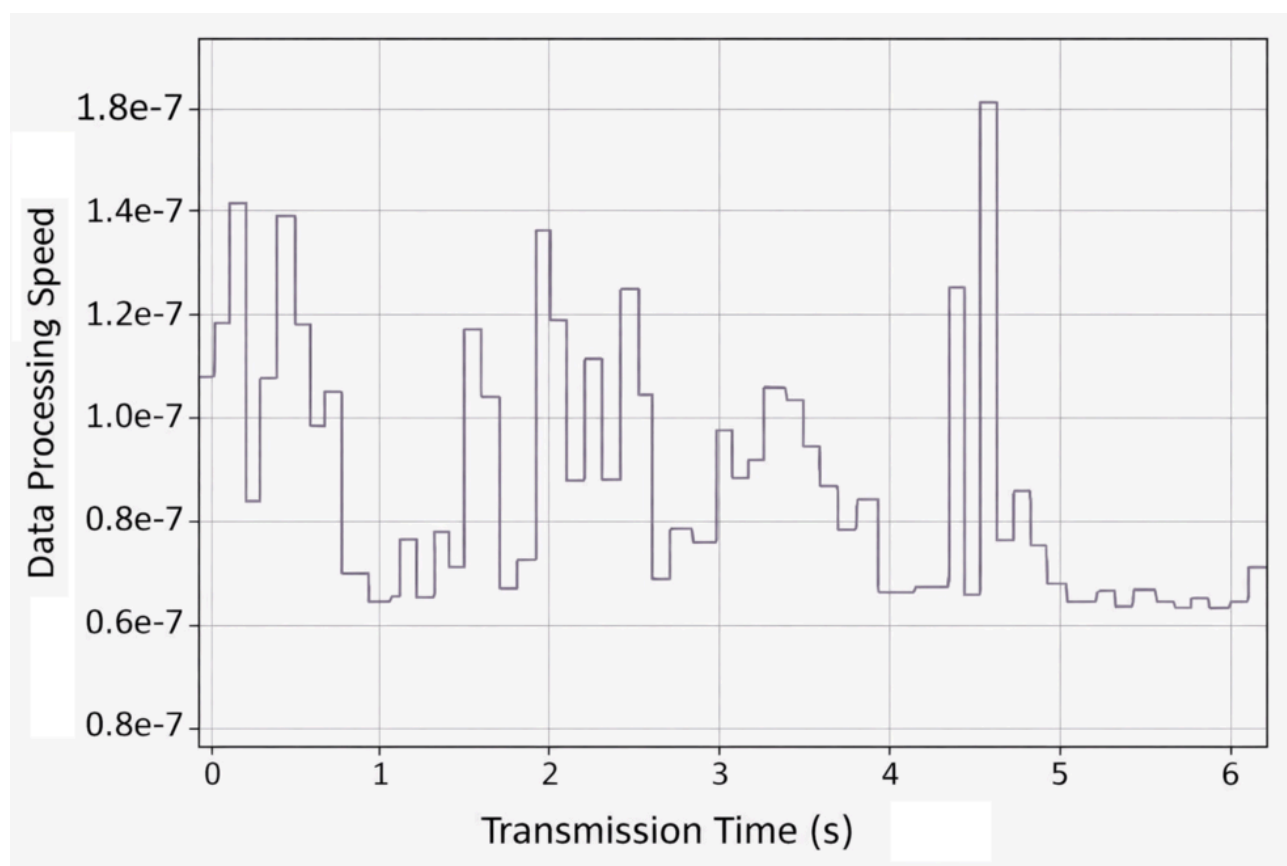


FIGURE 8: Time required to update health records.

The time required to update health records in both blockchain-based and traditional systems is compared in Figure 8. The graphic shows how long it takes to update medical records using both the blockchain-based healthcare model and the traditional client/server architecture. The execution durations are displayed for varying numbers of medical records, demonstrating a clear relationship between processing time and record count. A comparative performance evaluation of different cryptographic algorithms used for data security is illustrated in Figure 9. For both models, the execution time grows linearly with the number of records. However, as compared to the blockchain-based paradigm, the client/server architecture exhibits quicker execution. This discrepancy is explained by the blockchain's dependence on a consensus process for data replication and validation. All participating hospitals receive updated medical records and a duplicate ledger for verification when using the blockchain method. To ensure that everyone in the network agrees on its inclusion in the ledger, each peer node also communicates the hash of the revised block to the other nodes. Although these procedures improve data security and integrity, they also lengthen the blockchain model's execution time.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

Cryptographic algorithm	Encryption time (ms)	Decryption time (ms)	Key size (bits)	Throughput (Mbps)
AES (128-bit)	0.03	0.03	128	1500
RSA (2048-bit)	500	450	2048	0.8
RSA (4096-bit)	1000	950	4096	0.4
Lattice-based (Post-Quantum)	2500	2400	2048	0.2
Hybrid (AES + RSA)	0.35	0.3	128+2048	800

TABLE 1: Performance metrics for cryptographic algorithms in EHR security.

AES: advanced encryption standard; EHR, electronic health record; RSA, Rivest-Shamir-Adleman algorithm; SHA, secure hash algorithm.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

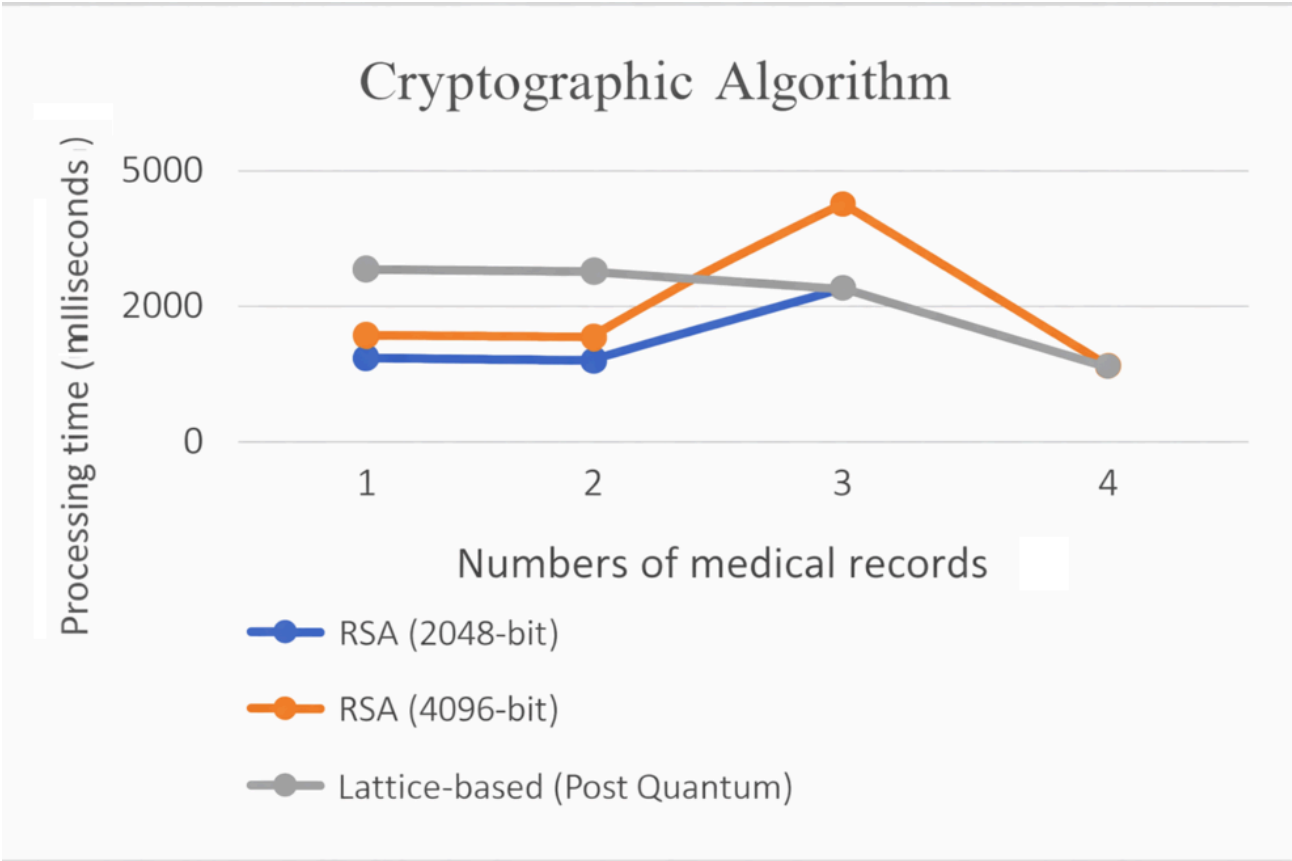


FIGURE 9: Performance of different cryptographic algorithms used in securing data.
RSA, Rivest-Shamir-Adleman algorithm.

The performance metrics of various cryptographic algorithms used in EHR security are summarized in Table 7. AES (128-bit) is the fastest algorithm, with minimal encryption and decryption times, making it highly suitable for high-throughput applications (1500 Mbps). RSA, with key sizes of 2048-bit and 4096-bit, offers strong security but comes at the cost of significantly higher encryption and decryption times [500 millisecond (represented as ms) and 450 ms for 2048-bit, 1000 ms and 950 ms for 4096-bit], resulting in much lower throughput (0.8 Mbps and 0.4 Mbps, respectively). Lattice-based post-quantum encryption, designed to withstand quantum attacks, is much slower, with encryption and decryption times of 2500 ms and 2400 ms, and a low throughput of 0.2 Mbps, although it offers robust security against quantum threats. The hybrid AES + RSA approach balances speed and security, with moderate encryption/decryption times (0.35 ms and 0.3 ms) and a throughput of 800 Mbps, benefiting from the fast AES encryption combined with the security of RSA encryption.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

Security technique	Transaction time (ms)	Transaction throughput (TPS)	Data integrity check time (ms)
Blockchain (SHA-256 + RSA)	200	10	50
Blockchain (SHA-256 + ECDSA)	180	12	40
Blockchain (Hybrid AES + RSA)	150	15	30
Blockchain (Lattice-based)	300	8	80
Blockchain (Post-Quantum + Hybrid)	350	6	90

TABLE 2: Comparison of blockchain transactions in EHR systems with different security techniques.

AES: advanced encryption standard; ECDSA, Elliptic Curve Digital Signature Algorithm; EHR, electronic health record; RSA, Rivest-Shamir-Adleman algorithm; SHA, secure hash algorithm.

A comparison of blockchain transaction performance under different security techniques is presented in Table 2, focusing on transaction time, transaction throughput (TPS), and data integrity check time. The performance of EHR systems employing different security techniques is summarized in Figure 10. The Blockchain with SHA-256 + RSA offers moderate transaction time (200 ms) and throughput (10 TPS), with a data integrity check time of 50 ms. The Blockchain with SHA-256 + ECDSA performs slightly faster, reducing the transaction time to 180 ms and improving throughput to 12 TPS, while data integrity checks take 40 ms. The hybrid AES + RSA blockchain improves performance further, with the fastest transaction time of 150 ms, the highest throughput at 15 TPS, and the lowest data integrity check time of 30 ms. In contrast, the Blockchain using Lattice-based encryption, while more secure against quantum attacks, results in slower performance with 300 ms transaction time, lower throughput (8 TPS), and higher data integrity check time (80 ms). The Post-Quantum + Hybrid blockchain, designed for post-quantum security, offers the slowest performance, with a transaction time of 350 ms, the lowest throughput (6 TPS), and the longest data integrity check time (90 ms).

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

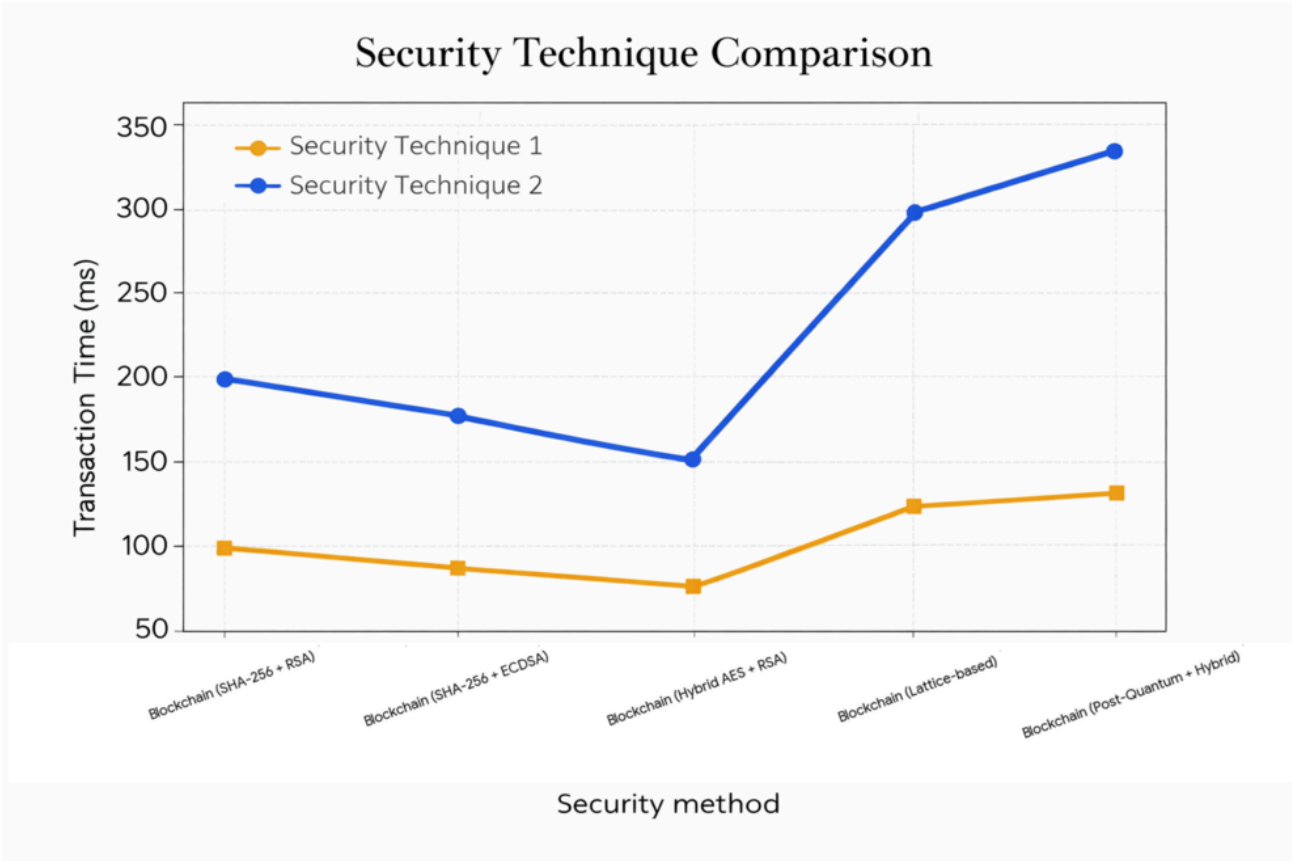


FIGURE 10: EHR systems with different security techniques.
AES: advanced encryption standard; ECDSA, Elliptic Curve Digital Signature Algorithm; EHR, electronic health record; RSA, Rivest-Shamir-Adleman algorithm; SHA, secure hash algorithm.

Blockchain security approach	Nodes (number of systems)	Block verification time (ms)	Transaction finality (seconds represented as s)	Network latency (ms)
SHA-256 + RSA	100	200	5	50
(AES + RSA)	150	150	3	45
Lattice-based	50	400	8	100
AES + Post-Quantum RSA	80	350	7	90

TABLE 3: Blockchain system scalability in healthcare (EHR systems).

AES: advanced encryption standard; EHR, electronic health record; RSA, Rivest-Shamir-Adleman algorithm; SHA, secure hash algorithm.

The scalability characteristics of blockchain-based healthcare systems are analyzed in Table 3. This compares different blockchain security approaches based on the number of nodes, block verification time, transaction finality, and network latency. The scalability of blockchain-based EHR systems under different security approaches is analyzed in Figure 11. The SHA-256 + RSA approach with 100 nodes has a block verification time of 200 ms, transaction finality of 5 s, and network latency of 50 ms. The AES + RSA approach, utilizing 150 nodes, performs faster with a block verification time of 150 ms, reduces transaction finality to 3 s, and offers lower network latency (45 ms). The Lattice-based approach, which focuses on quantum-resistant security, uses 50 nodes but has the longest block verification time (400 ms), a slower transaction finality of 8 s, and a higher network latency of 100 ms. The AES + Post-Quantum RSA approach, with 80 nodes, has a block verification time of 350 ms, transaction finality of 7 s, and network latency of 90 ms. Overall, AES + RSA provides the best performance in terms of verification time, finality, and latency.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

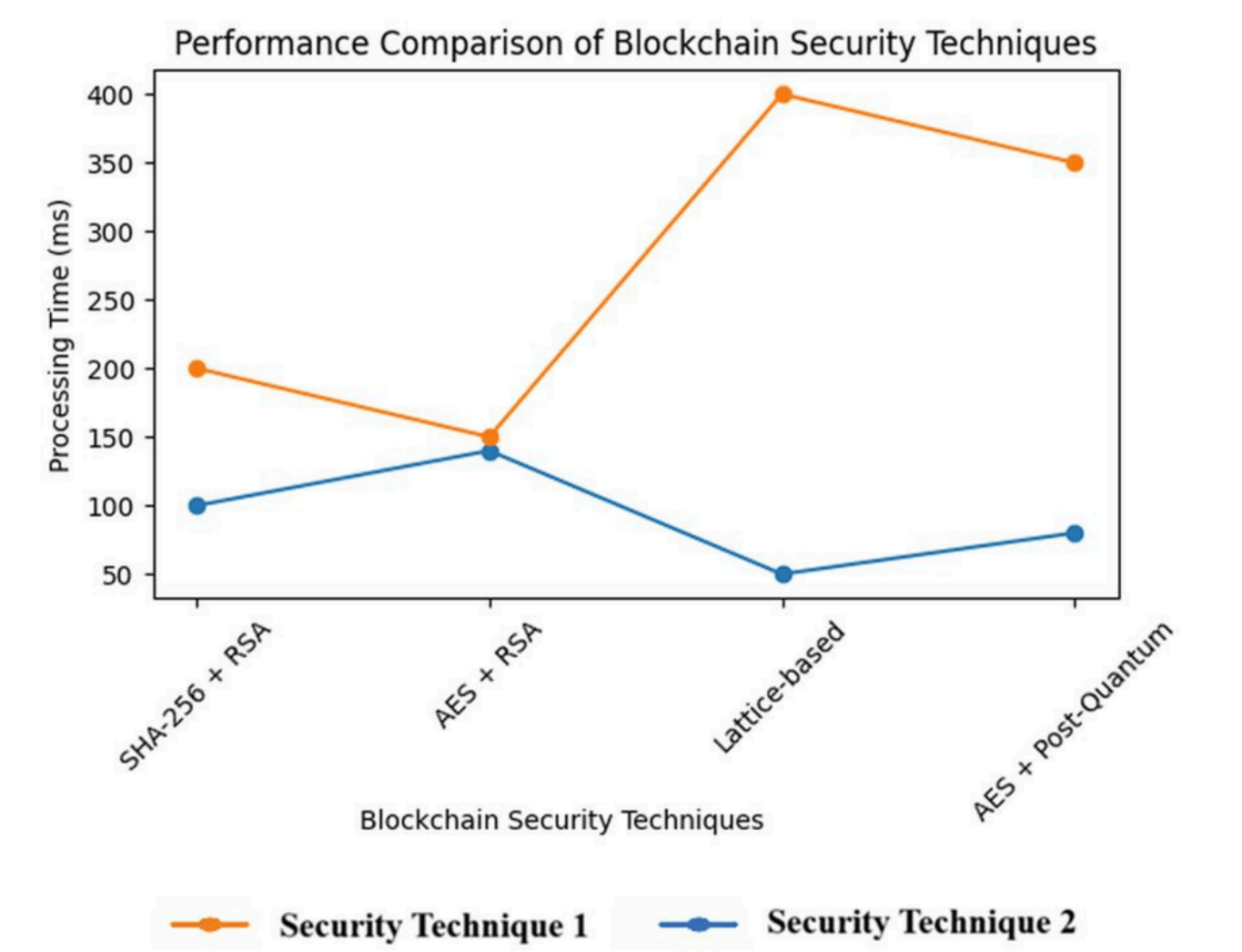


FIGURE 11: Performance comparison of blockchain security techniques.
AES: advanced encryption standard; Rivest-Shamir-Adleman algorithm; SHA, secure hash algorithm.

Discussion

The experimental analysis confirms that the proposed blockchain-based hybrid encryption framework successfully balances security, performance, and scalability. While post-quantum cryptographic mechanisms introduce additional overhead, the hybrid design minimizes performance penalties while ensuring resistance against future quantum threats. The results validate the framework’s feasibility for secure, decentralized EHR management and demonstrate its readiness for deployment in next-generation healthcare systems.

The proposed framework for safeguarding electronic health data using blockchain-based hybrid encryption and anti-quantum signature approaches enables further advancements in quantum-resilient cryptographic systems. Continuous innovation is essential to guarantee the resilience, scalability, and applicability of such frameworks across all areas as the danger of quantum computing approaches. The framework would be able to manage the growing need for safe, real-time processing of EHRs with this improvement. Long-term security requires the use of quantum-resilient methods. Although the hybrid signature system that combines Dilithium and ECDSA seem promising, further investigation into

different post-quantum cryptography methods is necessary. It is important to evaluate the applicability, security, and efficacy of hash-based signatures, multivariate polynomial-based algorithms, and lattice-based encryption for blockchain systems.

Conclusions

This study presents a novel approach to enhancing the security of EHRs through the use of quantum-resilient blockchain technology. By combining the efficiency of ECDSA with the quantum resistance of Dilithium, the proposed hybrid encryption architecture offers a robust defense for EHRs against the new threats posed by quantum computing. The system's integration of QBS significantly strengthens the integrity and privacy of sensitive health data by preventing hostile actors from manipulating or forging transactions. The findings demonstrate that the suggested method is viable for real-world healthcare applications as it retains computing economy while offering a high degree of security. Furthermore, a safe and decentralized environment for EHR administration is made possible by the system's scalability, which guarantees that it may be deployed across many healthcare networks. This breakthrough opens the door to more robust and secure healthcare data systems as quantum computing develops. In order to keep blockchain-based EHR systems safe in a society that is becoming more and more conscious of quantum issues, future research can concentrate on improving the framework's scalability and investigating other post-quantum cryptography techniques.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Harish P. Bhabad, Anand Singh Rajawat

Acquisition, analysis, or interpretation of data: Harish P. Bhabad, Anand Singh Rajawat

Drafting of the manuscript: Harish P. Bhabad, Anand Singh Rajawat

Critical review of the manuscript for important intellectual content: Harish P. Bhabad, Anand Singh Rajawat

Supervision: Anand Singh Rajawat

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

Data Availability Statements

The datasets (and/or code) supporting this study are available from the corresponding author upon reasonable request. All data generated or analyzed during this study are included in this published article and/or its appendices.

References

1. Usman M, Qamar U: [Secure electronic medical records storage and sharing using blockchain technology](#). *Procedia Computer Science*. 2020, 174:321-327. [10.1016/j.procs.2020.06.093](https://doi.org/10.1016/j.procs.2020.06.093)

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. *Cureus J Comput Sci* 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

2. Fiore M, Capodici A, Rucci P, et al.: [Blockchain for the healthcare supply chain: a systematic literature review](#). Applied Sciences. 2023, 13:686. [10.3390/app13020686](#)
3. Javaid M, Haleem A, Singh RP: [Health informatics to enhance the healthcare industry's culture: an extensive analysis of its features, contributions, applications and limitations](#). Informatics and Health. 2024, 1:123-148. [10.1016/j.infoh.2024.05.001](#)
4. Ismail S, Reza H: [Security challenges of blockchain-based supply chain systems](#). 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2022, 1-6. [10.1109/UEMCON54665.2022.9965682](#)
5. Sifra EM: [Security vulnerabilities and countermeasures of smart contracts: a survey](#). IEEE International Conference on Blockchain (Blockchain), Espoo, Finland. 2022, 512-515. [10.1109/Blockchain55522.2022.00080](#)
6. Haleem A, Javaid M, Singh RP, Suman R, Rab S: [Blockchain technology applications in healthcare: an overview](#). International Journal of Intelligent Networks. 2021, 2:130-139. [10.1016/j.ijin.2021.09.005](#)
7. Alves CJRA, dos Anjos FEV, Costa CA, Sellitto M, da Silva DO: [A review of blockchain modeling and proposals inside healthcare](#). Blockchain: Research and Applications. 2026, 100441. [10.1016/j.bcr.2026.100441](#)
8. Sehim K, Bendaoud F, Benderbal HH: [A review of scalability solutions in blockchain-based electronic health record systems](#). International Conference on Networking, Sensing and Control (ICNSC), Marseille, France. 2023, 1-6. [10.1109/ICNSC58704.2023.10319026](#)
9. Gong Y, Chang X, Mišić J, Mišić VB, Wang J, Zhu H: [Practical solutions in fully homomorphic encryption: a survey analyzing existing acceleration methods](#). Cybersecurity. 2024, 7:1-23. [10.1186/s42400-023-00187-4](#)
10. Cherkaoui DK, Tasic I, Cano MD: [Exploring post-quantum cryptography: review and directions for the transition process](#). Technologies. 2024, 12:241. [10.3390/technologies12120241](#)
11. Mafike SS, Mawela T: [An enterprise framework for blockchain interoperability](#). Electronic Markets. 2026, 36:1-22. [10.1007/s12525-025-00869-6](#)
12. Leong WY, Leong YZ: [Enhancing blockchain security](#). IEEE Symposium on Wireless Technology & Applications . 2024, 108-112. [10.1109/ISWTA62130.2024.10651753](#)
13. Chen, Wei Z, Jia X, Zheng P, Han M, Yang X: [Current status and prospects of blockchain security standardization](#). IEEE 9th International Conference on Cyber Security and Cloud Computing. 2022, 24-29. [10.1109/CSCloud-EdgeCom54986.2022.00014](#)
14. Chen M, Zhang K, Zhang D, Yuan L: [Design of network security data exchange management system based on blockchain](#). International Conference on Telecommunications, Electronics and Informatics. 2023, 506-510. [10.1109/ICTEI60496.2023.00064](#)
15. Bhutta MNM, Khwaja AA, Nadeem A, et al.: [A survey on blockchain technology: evolution, architecture and security](#). IEEE Access. 2021, 9:61048-61073. [10.1109/access.2021.3072849](#)
16. Leng J, Zhou M, Zhao JL, Huang Y, Bian Y: [Blockchain security: a survey of techniques and research directions](#). IEEE Transactions on Services Computing. 2020, 15:2490-2510. [10.1109/tsc.2020.3038641](#)
17. Singh S, Hosen ASMS, Yoon B: [Blockchain security attacks, challenges, and solutions for the future distributed IoT network](#). IEEE Access. 2021, 9:13938-13959. [10.1109/access.2021.3051602](#)
18. Khan R, Mehmood A, Maple C, Curran K, Song HH: [Performance analysis of blockchain-enabled security and privacy algorithms in connected and autonomous vehicles: a comprehensive review](#). IEEE Transactions on Intelligent Transportation Systems. 2023, 25:4773-4784. [10.1109/tits.2023.3341358](#)
19. Essaid M, Ju H: [Blockchain solutions for enhancing security and privacy in industrial IoT](#). Applied Sciences. 2025, 15:6835-6835. [10.3390/app15126835](#)
20. Li G, Dong M, Yang LT, Ota K, Wu J, Li J: [Preserving edge knowledge sharing among IoT services: a blockchain-based approach](#). IEEE Transactions on Emerging Topics in Computational Intelligence. 2020, 4:653-665. [10.1109/tetci.2019.2952587](#)
21. Zuo Y, Kang Z, Xu J, Chen Z: [BCAS: A blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing](#). International Journal of Distributed Sensor Networks. 2021, 17:155014772199961. [10.1177/1550147721999616](#)
22. Al-Nbhany WANA, Zahary AT, Al-Shargabi AA: [Blockchain-IoT healthcare applications and trends: a review](#). IEEE Access. 2024, 12:4178-4212. [10.1109/access.2023.3349187](#)
23. Menezes AJ, van Oorschot PC, Vanstone SA: [Handbook of Applied Cryptography](#). CRC Press, Boca Raton; 1997.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>

24. Linke B. Using the Elliptic Curve Digital Signature Algorithm Effectively. (2014). Accessed: January 30, 2026: <https://www.embedded.com/using-the-elliptic-curve-digital-signature-algorithm-effectively>.

How to cite this article:

Bhabad H P, Rajawat A (May 22, 2026) Enhancing Blockchain Security for Electronic Health Records with Hybrid Encryption and Anti-Quantum Signatures. Cureus J Comput Sci 3 : es44389-026-00080-4. DOI <https://doi.org/10.7759/s44389-026-00080-4>