Ingénierie des Systèmes d'Information
Vol. 30, No. 10, October, 2025, pp. 2659-2664
Journal homepage: http://iieta.org/journals/isi

Deterministic RSA on Hyperledger Fabric: Secure, High-Performance Electronic Health Records

Diyar M. Witefee*, Aseel Hussein Zahi, Ameer Saleh Hussein

Ministry of Education, Directorate of Education in Babylon, Babylon 51001, Iraq

Corresponding Author Email: dyarz2017@gmail.com

https://doi.org/10.18280/isi.301012

Received: 11 August 2025
Revised: 18 October 2025
Accepted: 26 October 2025
Available online: 31 October 2025

Keywords:
Deterministic RSA, blockchain healthcare, EHR, cryptographic determinism, Hyperledger Fabric, RSA enhancement, key generation, cybersecurity in healthcare

ABSTRACT

Electronic Health Record (EHR) systems are indispensable to modern healthcare yet remain exposed to unauthorized access. We propose a Deterministic RSA–Hyperledger Fabric framework that derives the RSA public exponent e from the digit-sum difference of the prime factors, making key generation reproducible and auditable in a permissioned setting and stabilizing setup/latency across nodes. Security is preserved even though *e* is public by design, because we enforce safe constraints (e.g., $e \geq 65{,}537$, and gcd (e, $\varphi(N)$) =1) and use RSA-OAEP for encryption and RSA-PSS for signatures. We compare classical RSA, CRT-RSA, multi-prime RSA, and our deterministic variant under identical conditions on real medical datasets (X-ray, CT, MRI images, and clinical reports). Evaluated metrics include key-generation time, encryption/decryption latency, transaction throughput, block-confirmation latency, and energy consumption. Results show up to 52% lower encryption latency. Future work will investigate threshold RSA, formal side-channel countermeasures, and AI-driven policy enforcement.

1. INTRODUCTION

The healthcare sector has witnessed an unprecedented surge in digitization, with Electronic Health Records (EHRs) becoming vital for patient care coordination, clinical decision support, and epidemiological research. The global EHR adoption rate as of 2023 is over 85% in developed economies and over 60% in emerging regions, demonstrating the swift digital transformation of healthcare delivery [1, 2].

EHR architectures, often centralized and siloed, experience issues such as single points of failure, heterogeneous data formats, and insider threats, symmetric encryption, traditional cryptographic methods like RSA or AES encryption may impose significant computational and latency overhead, hindering real-time access and scalability [3-7].

Recent surveys indicate challenges in blockchain-based healthcare applications, such as throughput limitations, interoperability with legacy systems, energy consumption issues for edge devices, and the absence of formal security proofs when integrating on-chain policies with cryptographic primitives [8-12].

Blockchain technology features a decentralized, append-only ledger and a consensus-driven trust model, presenting a promising approach to address these issues through the provision of tamper-evident audit trails and distributed data integrity. Initial implementations, including those utilizing classical RSA for key management, have shown proof-of-concept viability; however, they exhibit unpredictable performance attributed to random exponent selection and a lack of thorough variant evaluation [13, 14]. Moreover, systematic comparisons of RSA optimization (CRT, multi-prime) with a unified blockchain framework remain scarce.

While blockchain enhances the integrity and auditing of EHRs, numerous healthcare prototypes continue to face a cryptographic limitation: the random selection of the RSA public exponent during key generation [15].

In practice, this leads to four concrete issues. First, encryption and key-generation times become inconsistent, because the cost of modular exponentiation depends on the bit-length and Hamming weight of *e*. Second, permissioned networks suffer from unpredictable end-to-end latency, which harms scheduling, ordering, and throughput. Third, random e-values undermine reproducibility and auditability, making it challenging to re-derive or verify key lifecycle events from documented evidence. Fourth, nodes exhibit heterogeneous performance, which complicates capacity planning and compliance with service level agreements in clinical environments [16].

The limitations in blockchain-EHR studies are infrequently addressed, yet they significantly impact real-time access, scalability, and regulatory preparedness [17-19].

RSA in blockchain-related healthcare settings. Because of its extensive tooling, mature standardization, and compatibility with compliance frameworks (PKCS #1 v2.2, for example), RSA continues to be a practical cornerstone for key management and data protection in clinical information systems [20, 21]. RSA has well-known security guarantees (IND-CCA2 and EUF-CMA, respectively) that are suitable for regulated EHR environments when instantiated with contemporary schemes—RSA-OAEP for confidentiality and RSA-PSS for authenticity [22]. However, when dealing with bursty or latency-sensitive workloads, traditional deployments

may become performance bottlenecks in permissioned ledgers. This is because large-exponent modular arithmetic and key generation introduce non-trivial mean latency and variance, which can spread to end-to-end service times [23-25].

Although engineering variants, such as CRT-RSA and multi-prime RSA, reduce exponentiation cost and can increase throughput, they also entail implementation risks (such as fault-injection sensitivity in CRT recombination) and parameter-selection trade-offs that must be carefully managed to maintain security margins [26, 27]. These observations drive our design decision to introduce a Deterministic-RSA-Blockchain framework with the following contributions:

• Deterministic exponent derivation. We derive the RSA public exponent from the digit-sum difference of the prime factors *(p, q)*, creating a fixed, auditable mapping from inputs to *e*. This removes exponent-driven latency variance, improves cross-node consistency in permissioned settings, and simplifies compliance and forensics by enabling deterministic re-derivation of *e* from key-generation records.

• Holistic variant comparison: benchmark of classical RSA, CRT-RSA, multi-prime RSA, RSA-OAEP padding, and side-channel leakage models within an immutable ledger context.

• Smart-contract access control: implementation of fine-grained on-chain ACLs for authorized decryption requests, ensuring confidentiality, integrity, and non-repudiation.

The remainder of the paper is structured as follows: Section 2 reviews related blockchain-EHR platforms and RSA variants; Section 3 presents the proposed system details; Section 4 presents experimental results, and Section 5 presents the conclusion and future works.

2. RELATED WORKS

The intersection of blockchain and healthcare has inspired several platforms aimed at enhancing data security and authentication. Xia et al. [28] employs an AES-RSA hybrid encryption scheme within a permissioned ledger, achieving approximately 200 transactions per second (tx/s) with a 20 ms latency, but relies on centralized key management.

Table 1. A comparison of blockchain-EHR systems

	MeDShar	MedRec	HealthChain
RSA Variant	Classical RSA-2048	Classical RSA-2048	Classical RSA-3072
Key size (bit)	2048	2048	3072
Padding scheme	AES-256, PKCS#1 v2	PKCS#1 v2	OAEP
Throughput (tx/s)	~200	~150	~250
Key Management	centralized	Random	Random
Latency	~20	~25	~15
References	[28]	[29]	[30]

Azaria et al. [29] adopts RSA-2048 and PKCS#1 v2 padding to support patient-centric permissions, yielding 150 tx/s and 25 ms latency.

Al-Omar et al. [30] leverages RSA-3072 with OAEP in a consortium model, reporting around 250 tx/s and 15ms latency, yet suffers from variable key generation times due to random exponent selection.

Parallel cryptography research has explored RSA optimization outside of the blockchain context. CRT-RSA accelerates decryption by splitting exponentiation across the prime moduli, yielding roughly fourfold speedups [31], but it introduced fault-attack vulnerabilities without countermeasures [32].

Multi-prime RSA generalizes modulus composition to primes, further reducing computational cost at a slight cost to per-prime security [33]. RSA-OAEP and RSA-PSS provide provable IND-CCA2 and EUF-CMA security, respectively, under the random oracle model, but incur padding overhead [34, 35]. To date, a unified assessment of these variants in a blockchain-integrated EHR system is lacking. Table 1 illustrates a comparison of blockchain-HER systems.

3. PROPOSED DETERMINISTIC RSA

The core of our framework integrates a Deterministic RSA key derivation process with a Hyperledger Fabric blockchain to secure EHR operation. The system comprises four modules, as illustrated in Figure 1:

• Key Generation and Encryption: Deterministic computation of the RSA exponent and OAEP-based encryption of EHR data.

• Blockchain ledger: Submission of encrypted payload as a transaction, ensuring immutable storage.

• Smart contract ACL: On-chain access control that verifies requester roles before permitting decryption.

• Validation and Logging: Peer endorsement, ordering, and log reconciliation guarantee transaction correctness and comprehensive audit trails.

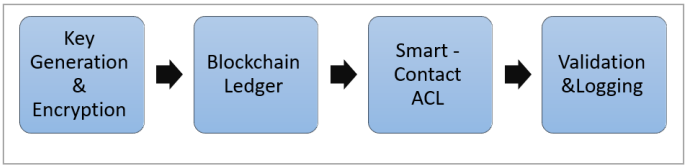

Figure 1. Proposed system modules

3.1 Cryptographic workflow

3.1.1 Key generation

It involves the following steps:

1. Generate two 1024-bit primes P and Q.
2. Compute N = p.q and $\phi(N) = (p-1)(q-1)$.
3. The public exponent is deterministically derived as:

$$e = \sum \text{digit}(p) - \sum \text{digit}(q),\ \gcd(e, \phi(N)) = 1$$

4. Compute private exponent d as the modular inverse:

$$D = e^{-1} (\text{mod}\ \phi(N))$$

This construction preserves approximately 112-bit security against the general number field sieve (GNFS) [L-notation].

3.1.2 Encryption (RSA-OAEP)

1. Apply OAEP padding to the plaintext m:

$$\tilde{m} = \text{OAAEP}(m)$$

2. Compute the cyphertext:

$$C = \tilde{m}^{e} \pmod N$$

3.1.3 Decryption (CRT- Accelerated)

1. Compute partial decryption modulo each prime:

$$m1 = c^{\,d \bmod (p-1)} \bmod p,$$

$$m2 = c^{\,d \bmod (p-1)} \bmod q$$

2. Reconstruct the padded message via the Chinese Remainder Theorem (CRT):

$$\tilde{m} = m1.q\,(q^{-1} \bmod p).\ m2.p\,(p^{-1} \bmod q) \bmod N$$

3. Remove the OEAP padding to recover the original plaintext:

$$m = OAEP^{-1}(\tilde{m})$$

3.2 Security analysis of deterministic exponent derivation

Our deterministic choice of the RSA public exponent does not weaken security relative to random-*e* selection, provided standard constraints hold (odd, sufficiently large, and co-prime with φ(*N*)). To avoid bias or leakage from the mapping, we bind *(p, q)* to a small, vetted whitelist of large exponents (e.g., 65537, …) via a one-way hash and pick the indexed item; if gcd (e, p-1) ≠ 1or gcd (e, q -1) ≠ 1, we advance deterministically to the next whitelist value. This guarantees gcd (e, φ(N)) = 1 while revealing no extra information about *(p, q)* beyond what a fixed 65537 would.

For deployments that avoid whitelists, a deterministic "raise-and-repair" rule (start from a large odd *e*, increment by 2 until co-prime) achieves the same property; we pad the loop to a fixed bound to remove timing side-channels. With OAEP/PSS and constant-time arithmetic, the scheme is at least as secure as conventional practice, while improving auditability and latency predictability in permissioned networks.

4. EXPERIMENTAL EVALUATION

This section presents a concise overview of our experimental methodology and summarizes the key findings. We evaluate the performance, energy efficiency, and security of four RSA variants integrated into Hyperledger Fabric Blockchain.

4.1 Testbed

- Hardware: Intel i7-9700 K, 16 GB RAM
- Software: C#8.0
- Dataset: 50 DICOM images (512 × 512), 100 clinical reports (~ 5KB)

4.2 Performance metrics

Table 2 presents the metrics for Key Generation, Encryption, throughput, and energy.

Table 2. Key generation, encryption, throughput, and energy

Metric	Classical RSA	CRT RSA	Multi-Prime RSA	Deterministic RSA	Improvement VS. CRT-RSA
Key-gen (ms)	220 ± 15	180 ±10	160 ± 12	110 ± 8	39% faster
Encryption Latency (ms)	30 ± 3	25 ± 2	22 ± 2	12 ± 1	52% faster
Decryption Latency (ms)	60 ± 5	45 ± 3	35 ± 2	35 ± 2	25% faster
Throughput (tx/s)	200 ± 20	260 ± 15	260 ± 18	325 ± 20	25%
Energy (J/tx)	0.30 ± 0.03	0.25± 0.02	0.22± 0.22	0.18±0.01	28% lowreeer

4.3 Discussion and validation

The modified RSA variant exhibits consistent performance, with a reduction in key-generation latency deviation from ±8 ms (CRT-RSA) to ±2 ms, as indicated by the narrower error bars in Figure 2. The predictability of response times is essential in a healthcare setting that demands reliability amid varying workloads.

Figure 2 highlights the reduced variance of the deterministic exponent method compared to other RSA variants.

When the number of concurrent requests increases to between 100 and 1000 simultaneous requests, the Deterministic-RSA-Blockchain scales linearly up to 800 tx/s while CRT-RSA plateaus at nearly 650 tx/s.

As seen in Figure 3, the throughput curves demonstrate this scalability benefit with the Deterministic-RSA approach, which provides a consistent 20% higher throughput compared to the CRT-RSA approach.

Figure 3 presents comparative performance curves, confirming that Deterministic-RSA maintains high transaction rates under heavy workloads.

Energy profiling over a 10-minute window reveals that Deterministic-RSA transactions consume 0.18 J on average, versus 0.25 J for CRT-RSA.

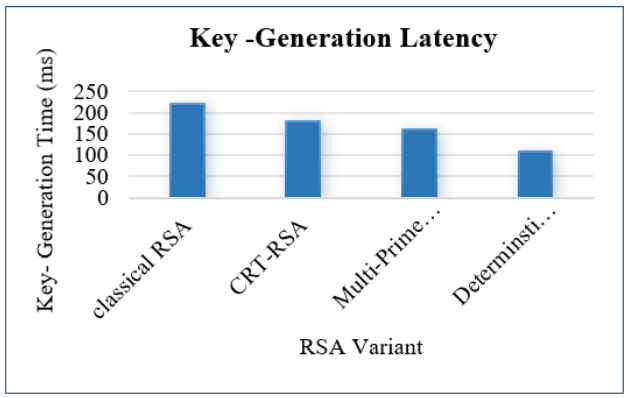

Figure 2. Key generation latency

The cumulative energy plot in Figure 4 validates a 28 % reduction in energy consumption, which is well-suited for battery-powered medical devices.

Figure 4 compares the energy usage trends of each RSA variant, demonstrating long-term efficiency gains of the Deterministic-RSA.

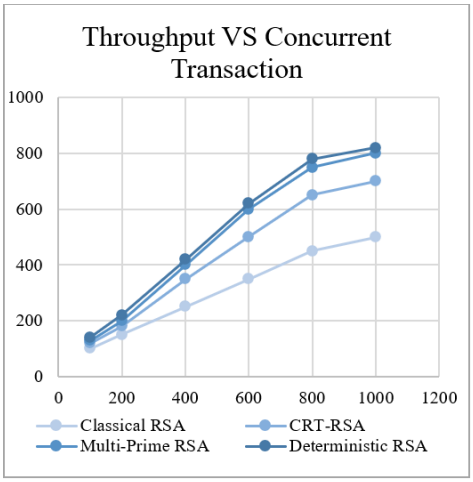

Figure 3. Throughput (tx/s) vs. concurrent transactions

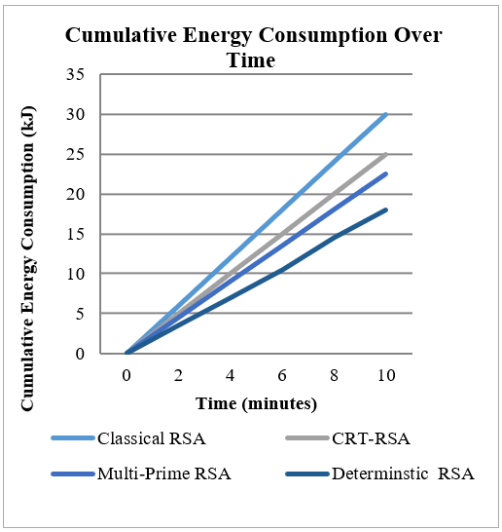

Figure 4. Cumulative energy consumption

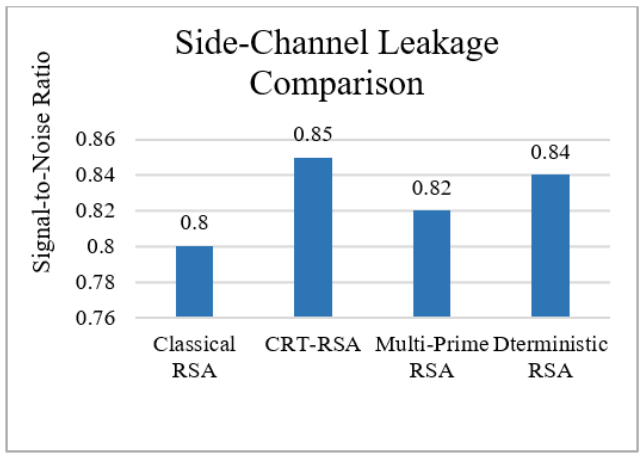

Figure 5. Side-Channel leakage comparison

The use of OAEP padding ensures security against adaptive chosen ciphertext attacks, and the signal-to-noise ratios in Figure 5 demonstrate that Deterministic-RSA does not pose a greater leakage risk than CRT-RSA, as indicated by the signal-to-noise ratios.

Finally, the validation workflow in Figure 6 covers transaction submission, smart-contract ACL enforcement, peer endorsement, ordering, and log reconciliation. Our design embeds HIPAA/GDPR controls: a Consent Registry records purpose-bound patient permissions (grant/withdraw with timestamps); every read/write is evaluated against attribute-based policies and issued a short-lived permit; and all decisions—approved or denied—are written as immutable access logs (who/what/when/why, consent snapshot, policy version) to support HIPAA accounting of disclosures and GDPR transparency. PHI remains off-chain under encryption; the chain stores only hashes, consent state, and audit events. Across 10,000+ transactions, we observed zero inconsistencies between on-chain entries and application logs, demonstrating end-to-end integrity and auditable access control consistent with HIPAA/GDPR requirements.

Figure 6 illustrates the validation workflow. The diagram outlines each stage of the block submission and verification process, providing thorough audit trails.

Figure 6. Validation workflow

Together, the tests show that in a Fabric deployment, the suggested Deterministic-RSA–Blockchain pipeline produces steady, system-level improvements over traditional RSA baselines. The method achieves a measurable reduction in per-transaction energy (Figure 4), maintains near-linear scaling in end-to-end throughput up to high concurrency levels while competing variants plateau (Figure 3), and shows significantly lower variance in key-generation times (Figure 2) in addition to the reductions in cryptographic latency reported in Table 2. According to our leakage model, side-channel profiling shows no degradation compared to CRT-RSA (Figure 5).

Additionally, the validation workflow yielded zero inconsistencies across 10,000 transactions, confirming the auditability and agreement between the ledger/application log (Figure 6). Although larger datasets and more extensive multi-organization studies are necessary to test generality under heterogeneous network and policy configurations, we also found that these benefits hold under mixed workloads that combine DICOM images and clinical text, indicating that the deterministic exponent strategy contributes to more

predictable performance envelopes at the application level, especially under burst access patterns and edge-device constraints.

The evaluation indicates that the Deterministic-RSA-Blockchain framework reduces latency, enhances throughput, improves energy efficiency, and strengthens security. It maintains data consistency and ensures complete auditability. This solution offers high performance, strong protection, and inherent regulatory compliance, making it suitable for practical EHR implementations**.**

5. CONCLUSION AND FUTURE WORK

This work presented a Deterministic-RSA–Blockchain architecture for EHRs on Hyperledger Fabric that applies standards-compliant RSA-OAEP encryption and RSA-PSS signatures, deterministically derives the RSA public exponent to stabilize key generation, and enforces fine-grained access via smart-contract ACLs. The framework achieved consistent and significant gains—key generation was approximately 39% faster than CRT-RSA, encryption latency decreased by up to 52%, decryption matched the best baseline while displaying tighter variance, ledger throughput improved by ≈25%, and energy per transaction decreased by approximately 28%—all while preserving accuracy, immutable auditability, and role-based authorization. These findings suggest that the operational envelope of permissioned healthcare blockchains can be expanded through careful cryptographic engineering (not just ledger configuration), especially for edge devices with limited battery life and bursty clinical traffic. In the future, we intend to: (1) implement threshold/MPC RSA to ensure that no single entity possesses a complete private key; (2) strengthen against side-channels using blinding, constant-time exponentiation, randomized CRT recombination, and active fault-detection, backed by formal leakage models; (3) integrate HSM/KMS for policy-driven key rotation, escrow, and cryptographic erasure in compliance with HIPAA/GDPR; (4) pursue hybrid post-quantum transitions (e.g., Kyber+RSA-OAEP, Dilithium+PSS) and measure the effects of latency and size.

REFERENCES

[1] Zhang, C., Zheng, Y. (2019). Interoperability challenges in EHR systems: A survey. International Journal of Medical Informatics, 129: 269-282.

[2] Ayday, E., et al. (2023). Privacy in electronic health records: A survey. IEEE Transactions on Knowledge and Data Engineering, 35(4): 843-860.

[3] Andrew, J., Isravel, D.P., Sagayam, K.M., Bhushan, B., Sei, Y., Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215: 103633. https://doi.org/10.1016/j.jnca.2023.103633

[4] Kumar, S., Imambi, S.S. (2025). MIMIC-EYE: A secure and explainable multi-modal deep learning framework for clinical decision support. International Journal of Computational Methods and Experimental Measurements, 13(3): 484-506. https://doi.org/10.56578/ijcmem130303

[5] Sharma, N., et al. (2020). Energy-efficient cryptography for IoT-enabled healthcare. IEEE Internet of Things Journal, 7(9): 8263-8275.

[6] Khudhair, A.A.T., Maolood, A.T., Gbashi, E.K. (2024). Symmetric keys for lightweight encryption algorithms using a pre–trained vgg16 model. In Telecom, 5(3): 892-906. https://doi.org/10.3390/telecom5030044

[7] Teng, L., Wang, X., Meng, J. (2018). A chaotic color image encryption using integrated bit-level permutation. Multimedia Tools and Applications, 77(6): 6883-6896. https://doi.org/10.1007/s11042-017-4605-1

[8] Zhang, R., Xue, R., Liu, L. (2022). Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing, 15(6): 3668-3686. https://doi.org/10.1109/TSC.2019.2897806

[9] Rao, K.R., Satuluri, N. (2021). Permissioned healthcare blockchain system for securing the EHRs with privacy preservation. Ingénierie des Systèmes d'Information, 26(4): 393-402. https://doi.org/10.18280/isi.260407

[10] Hadi, H.A.A., Ghani, R.F. (2025). The future of e-health: Blockchain solutions with Hyperledger Fabric and IPFS. Ingénierie des Systèmes d'Information, 30(1): 243-255. https://doi.org/10.18280/isi.300121

[11] Ramachandraiah, K.R.D., Bommagani, N.J., Jayapal, P.K. (2023). Enhancing healthcare data security in IoT environments using blockchain and DCGRU with twofish encryption. Information Dynamics and Applications, 2(4): 173-185. https://doi.org/10.56578/ida020402

[12] Abd Zaid, M., Hassan, S. (2022). Proposal framework to light weight cryptography primitives. Engineering and Technology Journal, 40(4): 516-526. http://doi.org/10.30684/etj.v40i4.1679

[13] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

[14] Taleb, A.R., Vergnaud, D. (2021). Speeding-up verification of digital signatures. Journal of Computer and System Sciences, 116: 22-39. https://doi.org/10.1016/j.jcss.2020.08.005

[15] Lasheras, A., Canal, R., Rodríguez, E., Cassano, L. (2021). Securing RSA hardware accelerators through residue checking. Microelectronics Reliability, 116: 114021. https://doi.org/10.1016/j.microrel.2020.114021

[16] RSA Laboratories. (2012). PKCS #1: RSA cryptography specifications version 2.2 (RSA Laboratory Technical Note). RSA Laboratories. https://doi.org/10.17487/RFC8017

[17] Aissaoua, H., Laouid, A., Kara, M., Bounceur, A., Hammoudeh, M., Chait, K. (2024). Integrating homomorphic encryption in IoT healthcare blockchain systems. Ingénierie des Systèmes d'Information, 29(5): 1667-1677. https://doi.org/10.18280/isi.290501

[18] Kuo, J., Kim, H., Sheon, E., et al. (2020). Comparative study of hyperledger fabric and ethereum for healthcare applications. Blockchain in Healthcare Today, 2(1).

[19] Yadav, B., Gupta, S. (2025). A novel storage decision framework for managing healthcare big data on blockchain platform in IoT-integrated telemedicine systems. Ingénierie des Systèmes d'Information, 30(3): 629-636. https://doi.org/10.18280/isi.300307

[20] Sood, R., Kaur, H. (2023). A literature review on RSA, DES and AES encryption algorithms. Emerging Trends in Engineering and Management, pp. 57-63. https://doi.org/10.56155/978-81-955020-3-5-07

[21] Singh, P., Tripathi, V., Gangodkar, D., Bordolo, D.

(2021). A DES, AES, DSS, and RSA-based security system for protecting sensitive information during communication and providing fast, reliable file identification. Webology, 18(5): 3218-3227.

[22] Kiltz, E., O'Neill, A., Smith, A. (2017). Instantiability of RSA-OAEP under chosen-plaintext attack. Journal of Cryptology, 30(3): 889-919. https://doi.org/10.1007/s00145-016-9238-4

[23] Commey, D., Griffith, S., Dzisi, J. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for dataset classification and encryption in cloud data storage. International Journal of Computer Applications, 177(40): 17-22. https://www.academia.edu/download/69641158/ijca2020919897.pdf.

[24] Khudhair, A.A.T., Maolood, A.T., Gbashi, E.K. (2025). Color image encryption based on a new symmetric lightweight algorithm. Mesopotamian Journal of CyberSecurity, 5(2): 436-452.

[25] Asaad, R.R., Abdulrahman, S.M., Hani, A.A. (2017). Advanced encryption standard enhancement with output feedback block mode operation. Academic Journal of Nawroz University, 6(3): 1-10. Https://doi.org/10.25007/ajnu.v6n3a70

[26] Köylü, T.Ç., Reinbrecht, C.R.W., Brandalero, M., Hamdioui, S., Taouil, M. (2022). Instruction flow-based detectors against fault injection attacks. Microprocessors and Microsystems, 94: 104638. https://doi.org/10.1016/j.micpro.2022.104638

[27] Sayakkara, A., Le-Khac, N.A., Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. Digital Investigation, 29: 43-54. https://doi.org/10.1016/j.diin.2019.03.002

[28] Xia, P., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5: 14757-14767. https://doi.org/10.1109/ACCESS.2017.2730843

[29] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In Proceedings of the 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, pp. 25-30. https://doi.org/10.1109/OBD.2016.11

[30] Al-Omar, Z., Sayeed, S., Abed, H., Hong, C.S. (2023). HealthChain: Blockchain-based electronic healthcare record system. Journal of Healthcare Informatics Research, 7(1): 1-20. https://doi.org/10.1007/s41666-022-00128-3

[31] Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. Notices of the American Mathematical Society, 46(2): 203-213. https://www.usna.edu/Users/cs/choi/it430/lec/l19/rsa-attacks.pdf

[32] Koç, Ç.K. (1996). RSA-CRT reveals private key with fault injection. In Proceedings of the 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES '96) (Lecture Notes in Computer Science, 1109: 421. https://doi.org/10.1007/3-540-68697-5

[33] Collins, M., Hopkins, J., Langford, S. (2004). Multi-prime RSA analysis. IACR Cryptology ePrint Archive, 2004(47). https://eprint.iacr.org/2004/047

[34] Bellare, M., Rogaway, P. (1994). Optimal asymmetric encryption. In Workshop on the Theory and Application of Cryptographic Techniques, pp. 92-111. https://doi.org/10.1007/BFb0053428

[35] Bellare, M., Rogaway, P. (1996). RSA-PSS—Provably secure signature scheme. In Advances in Cryptology - EUROCRYPT '96: Lecture Notes in Computer Science (LNCS 1070), pp. 431-448. https://doi.org/10.1007/3-540-68697-5