Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 6, pp. 2477–2488
DOI : 10.47974/JDMSC-2754

Enhancing EHR interoperability and privacy through blockchain and post-quantum hybrid cryptography

G. Mahesh *
Renu Mishra †
Department of Computer Science & Engineering
Sharda School of Engineering and Technology
Sharda University
Greater Noida 201310
Uttar Pradesh
India

Abstract

The Electronic health data (EHRs) employed with benefits of interoperability, better patient care, and obeying laws of regulation like Health Insurance Portability and Accountability Act (HIPAA). Existing and popular regulations like Digital Information Security in Healthcare Act (DISHA) and the General Data Protection Regulation (GDPR) are susceptible to fragmented governance, unauthorized access, and manipulation due to traditional centralized effects. This study introduces a Blockchain-based Patient-Centric Hybrid (BCPCH) method that ensures safe, scalable, and legally acceptable health data interchange through the combination of post-quantum cryptography and dynamic permission management. This paper combines Kyber algorithm for key encapsuplation, Dilithium algorithm for authentication of patient data and Hierarchical Identity-Based Encryption (HIBE) for role-based control to achieve patient-centric authentication Hybrid cryptographic primitives like Dilithium, Kyber, and HIBE are used in this dual-layer architecture to enable encryption, well formed delegation, and quantum-resilient signatures. Smart contracts are utilized for role-based access control and immutability in the Blockchain.When compared to cryptographic algorithms, its results show the best throughput, scalability, post-quantum resistance, and future-ready path for patient-driven, safe, and lawful digital healthcare ecosystems. It also preserves interoperability, promotes patient-driven consent, and makes real-time permission and revocation easier.

Subject Classification: *94A60, 68P20.*

Keywords: *Interoperability, Patient-centric, Hybrid cryptography, Blockchain, Smart contracts, Post-quantum.*

* *E-mail:* **2022452915.mahesh@dr.sharda.ac.in (Corresponding Author)**
† *E-mail:* **renu.mishra@sharda.ac.in**

1. Introduction

Electronic Health Records (EHRs) became essential for clinical decision-making, care coordination, and patient-controlled data sharing. However, despite the adoption of standards such as FHIR and HL7, healthcare systems remain fragmented, leading to interoperability limitations and increased risks of unauthorized access and system failures. Standard Regulatories like HIPAA, GDPR, and DISHA further necessitate secure, and efficient healthcare data exchange mechanisms [1], [3]. Blockchain technology provides tamper-resistant, patient-centric access control and interoperable data sharing, with smart contracts ensuring consent enforcement, data integrity, and accountability [4], [5], [7], [16]. Nevertheless, existing blockchain-based EHR solutions face scalability constraints and rely on classical cryptographic algorithms like RSA, ECC, Deffie Hellman, which are vulnerable to quantum attacks [12], [19]. To address these challenges work contributed by this framework as follows : (i) proposing a patient-centered blockchain EHR system integrating quantum-safe algorithms with dynamic consent management, (ii) constructing a tiered architecture using ReactJS–Flask and IPFS-based decentralized storage, and (iii) comparing performance with classical cryptography in terms of throughput, scalability, and compliance [4], [5], [6]. As the result,comparison of the proposed framework performance are shown with classical cryptographical algorithms in terms of throughput, scalability, and compliance preparedness.

2. Related works

The various research studies resolved EHR issues of secure and interoperable sharing using blockchain, although, issues of consent management, scalability, quantum resilience and interoperability exist [27]. Edge- and IoMT-enabled research such as BEdgeHealth [13] and cooperative blockchain–edge architectures [15] resolved QoS and privacy through smart-contract-based authentication [11]. An Efficient and Privacy-Preserving Search algorithm over Encrypted Data is also implemented over the Blockchain [10]. Blockchain-Enabled Consent automation and access enforcement with Fine-Grained Searchable Encryption over Cloud are already discussed and defined briefly in FedBlockHealth [14], [18], and also patient-centric consent with real-time revocation is emphasized in [19], [20], [23], [25]. Current studies integrate post-quantum cryptography (PQC) for long-term security briefed

progressively, as described in telehealth and EHR preservation frameworks [21], [23]. More efforts integrated blockchain with cloud–edge optimization [22], [24] for HIPAA-compliant infrastructure chronic disease management [8], metaverse-based telemedicine [2], and HSM-backed [9] defined. Scalability, interoperability, dynamic consent, post-quantum security, and compliance validation remain issues for current blockchain-based EHR systems. Many are still pilot-scale, don't integrate with HL7/FHIR standards, or don't offer PQC methods that are ready for migration. A comparative analysis of the focus areas and limitations of these works is presented in Table 1 as shown below.

Table 1

Comparative analysis of limitation in existing papers

Reference	Focus	Features and Key Limitations
Kumari and Tewari [17]	Blockchain with iris scanning	Throughput minimized, variation in gas costs and lack of PQC integration .
Nguyen et al. [13]	Blockchain enabled by the IoMT	Reduces access time for healthcare files but no PQC support.
Rani et al. [15]	Blockchain-based cooperative sharing	computing resource sharing by integrating blockchain with wireless communication, no PQC support.
Purohit et al. [18]	Securing healthcare learning	Limited scalability concern, handling non Independent data,
Singh, Pippal, and Sharma [1]	Privacy with federated learning	No permission is dynamic, only pilot-scale
Agbo and Mahmoud [19], Hu et al. [20]	Management of Consent	Consent Primarily conceptual, devoid of hierarchical delegation and PQC.
Saini et al. [26]	Integration of PQC	PQC Limited adoption in the real world and no organized migration plans.
Chen, Chen, and Chen [2], Purohit et al. [9]	Domain-specific implementations	Concentrated on certain industries; insufficient generalization

These highlighted problems are addressed by the suggested BCPCH framework.

3. Proposed Architecture

The proposed BCPCH model based architecture is shown in Figure 1 which combines Kyber algorithm for key encapsuplation, Dilithium algorithm for authentication of patient data and HIBE for role-based control for patient-centric authentication along with the consent delegation for the authenticated doctors.

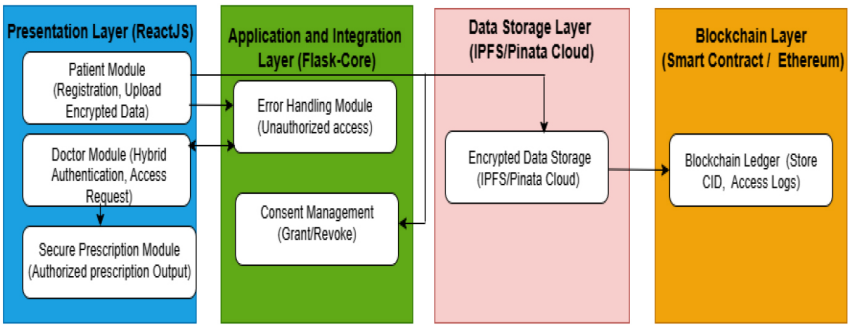

Figure 1

Blockchain-based patient-centered EHR management system

Dilithium and Kyber algorithms integration offer identity verification with quantum-resistant, secure key exchange between patient and authenticated staff with secured environment and communicate using blind sign and verify with public and private keys generated by HIBE, here public keys are derived from private keys, the patient information stored in IPFS by using piñata cloud and get the hash key for sharing to authenticated staff only with the assist of smart contract programming to achieve the role based control with relilience against the quantum-era hackers attack across the healthcare field. The implementation of model defined as revocable access control with the four layers design based architecture with involvement of functionalities such as presentation, application, decentralized storage and integration of blockchain with the properties of immutable audit, patient-centered dynamic consent management and post quantum computing defendant data sharing among healthcare stakeholders.

4. Working flow and Algoriths used

The flow of the proposed architecture can be depicted using below sequence diagram As shown in Figure 2, the encrypted patient record is

stored on blockchain through IPFS and get the corresponding hash key for future reference. These hash keys recorded in each block of blockchain. The patient can share the information for authenticated physicians with digitally signed communication with verifiable data sharing. Architecture prototype managed by the Ethereum with fronend tool ReactJS with backend server Flask microservices,implementation using Ethereum, ReactJS–Flask microservices.

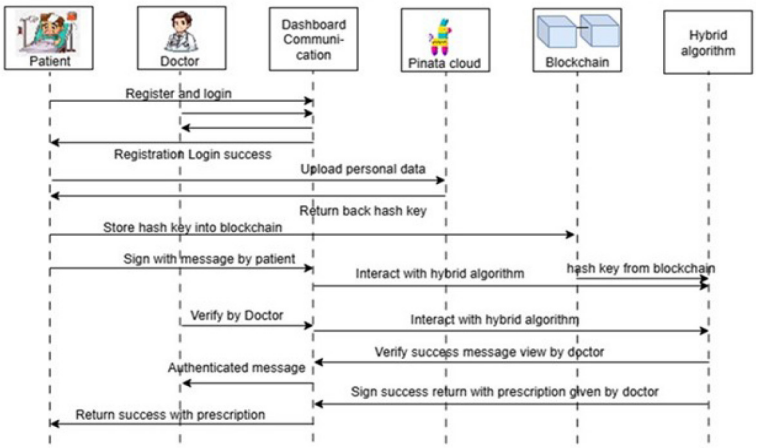

Figure 2

Sequence diagram with end-to-end workflow for BCPCH framework.

Algorithms 1-3 formalize the main procedures, which include finding doctors, distributing medications, and posting patient photos. Forward secrecy, patient-controlled authorization, and quantum-safe confidentiality preserved.

Algorithm 1. Upload of Patient Medical Images to IPFS and Blockchain.

Input: Medical image *I*
Output: Transaction hash *Tx_Hash* or Error

1. Generate session symmetric key *Ksym.*
2. Encrypt image C = $Enc_{sym}(I, K_{sym})$.
3. Upload C to IPFS via Pinata obtain hash key *Hipfs.*
4. IF H_ipfs = NULL then return Error: Upload failed
5. Prepare and submit blockchain transaction : *H_ipfs.*

6. Return transaction hash *Tx_Hash;* otherwise return failure.

Algorithm 2. Doctor Access of Patient Data with Patient Authorization

Input: Tx_Hash, Doctor_ID, PK_Dilithium_Doctor, SK_HIBE_Doctor, PK_Dilithium_Patient, Authorization_Proof
Output: Medical image *I* or Error

1. Retrieve blockchain transaction associated with *Tx_Hash.*
2. Verify patient Dilithium signature stored on IPFS with hashkey.
3. IF valid = false then return Error: Patient signature invalid
4. Verify doctor authorization:
   auth = Verify_Access(*Doctor_ID*, *Authorization_Proof*, *PK_Dilithium_Patient*)
5. IF auth = false then return Error: Unauthorized doctor
6. Download encrypted image and decrypt it.
   C = Pinata_API.Download(Tx["IPFS_hash"])
   I = Dec_sym(C, K_sym)
7. IF I = NULL then return Error: Image decryption failed
8. Return I

Algorithm 3. Secure Prescription Sharing by Doctor

Input: Prescription document *P*, Doctor_ID, PK_Dilithium_Doctor, SK_Dilithium_Doctor,PK_Dilithium_Patient, SK_Dilithium_Patient, Master Public Key MPK, Authorization_Proof, Communication channel CH
Output: Success or Error

1. Verify and validate doctor authentication
   auth = Verify_Dilithium(*PK_Dilithium_Doctor, Message Signature*)
   Verified=Verify_Access(*Doctor_ID, SK_Dilithium_Patient*, *Authorization_Proof*)
2. IF auth = false or verified=false then return Error: Doctor authentication or verification failed
3. Encrypt prescription key with HIBE:
   C_hibe = Enc_HIBE(*MPK*, *Patient_ID, K_sym_P*)

4. Sign prescription:
   Sig_P = Sign_Dilithium(*SK_Dilithium_Doctor, P*)
5. Prepare payload={Enc_sym, C_hibe, Sig_P, CurrentTime()}
6. Send payload via communication channel status = CH.SendToPatientDash board(Payload)
7. IF status = FAILED then return Error: failed else Prescription shared securely.

5. Experimental Result and Discussions

Results of the proposed BCPCH framework are analysed as described below.

5.1 *Experimental Hardware Testbed Setup.*

The proposed system is implemented blockchain of Docker-based and pinata cloud from IPFS services deployed via Ganache. Post-quantum primitives (Dilithium, Kyber, HIBE) were run by using the OQS library in Python, with benchmarking performed on Google Colab (Tesla T4 GPU).

5.2 *Throughput comparison of proposed model*

Table 2
Throughput comparison with traditional and proposed BCPCH model

Algorithms	Throughput (Ops/sec)	Justification
RSA	300	Lacks speed in processing data, which causes it to perform badly in healthcare applications.
DSA	350	Relatively modest throughput over RSA, which is insufficient to support several tasks concurrently.
DES	700	High processing speed, but its applicability is constrained by deployment and security concerns.
ECC	500	Enhanced throughput performance enables it to handle data at the mid-scale.
Proposed BCPCH	830	High transaction throughput while enabling efficient multi-party access in healthcare.

The proposed BCPCH model outperforms in terms of throughput and latency, which are crucial for blockchain-enabled healthcare systems as shown in Table 2 and Figure 3.

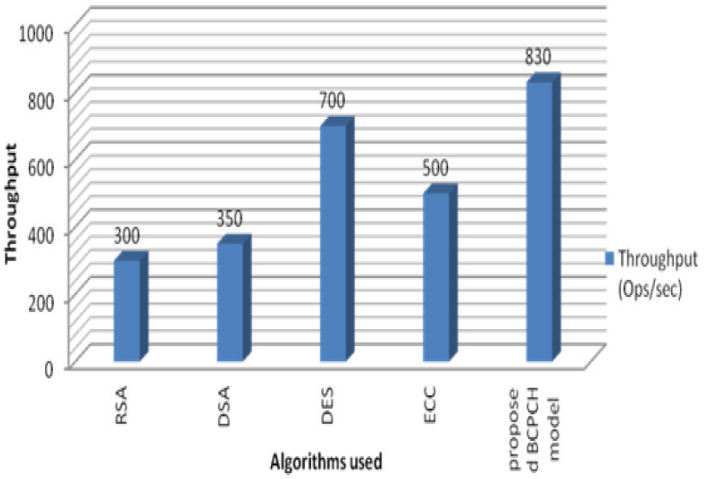

Figure 3

Throughput comparison of proposed vs. traditional algorithms

BCPCH ensures scalable, efficient, and patient-centric EHR operations, in contrast to conventional methods that are limited by speed, concurrency, or security.

5.3. *Comparison of Holistic Security and Comparative Performance with Baseline Systems*

Table 3 (a)

Throughput Performance under Varying Patient–Provider Ratios

Patient : Provider Ratio	Throughput (Transactions per Second)
10 : 50	200
50:20	400
100:50	650
200:100	800
500:200	950

Table 3 (b)

Comparative Evaluation of Cryptographic Schemes with proposed BCPCH model

Attribute / Scheme	Privacy	Forward Secrecy	Scalability	Compliance Readiness	Quan-tum Resis-tance
RSA	1.5	1.0	2.5	2.0	0.5
ECC	2.0	3.0	3.0	2.5	1.5
Dilithium	4.0	3.5	4.0	3.5	5.0
Kyber	4.5	4.0	4.0	4.0	5.0
Proposed BCPCH	5.0	4.5	4.5	4.5	5.0

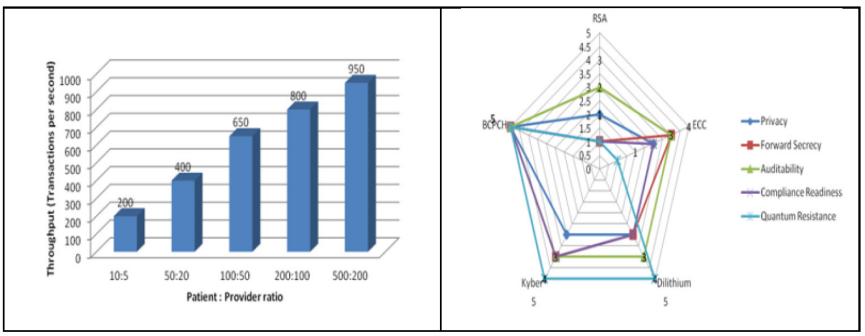

Figure 4 (a) and 4 (b)

Scalability of proposed model under Patient-Provider ratios

6. Discussion, Conclusion and Future scope

The Blockchain-based Patient-Centric Hybrid (BCPCH) framework resolves issues related with critical security, scalability and limitations of conventional EHR systems, which rely on classical public key infrastructure (PKI) and are vulnerable to quantum attacks. By collaborating post-quantum cryptographic primitives (Dilithium, Kyber, and HIBE) as shown in Table 3 (a) and 3 (b) and also through Figure 4 (a) and 4 (b) with blockchain immutability, scalable, secured and patient centric solution for next generation, the proposed model ensure for configurable access delegation, strong quantum resistance, and regulatory compliance. In future, more focus is recommended on formal verification of PQC modules and smart contracts, and real-world deployments to achieve interoperability, compliance, and sustainable adoption in healthcare.

References

[1] M. K. Singh, S. Kumar Pippal, and V. Sharma, "A Blockchain-IPFS framework for secure, scalable, and interoperable healthcare data management," *SN Computer Science*, vol. 6, no. 5 (2025), doi: 10.1007/s42979-025-03936-z.

[2] C. Chen, D. Chen, and E. Chen, "Blockchain and metaverse integration in telemedicine," *Journal of Healthcare Engineering*, vol. 2025, Art. no. 4734288 (2025), doi: 10.1155/2025/4734288.

[3] M. Pampattiwar and P. Chavan, "A secure and scalable blockchain-based model for electronic health record management," *Scientific Reports*, vol. 15, Art. no. 11612 (2025).

[4] M. Ben Othman and M. Getahun, "Leveraging blockchain and IoMT for secure and interoperable electronic health records," *Scientific Reports*, vol. 15, Art. no. 12358 (2025).

[5] O. Cheikhrouhou, K. Mershad, M. Laurent, and A. Koubaa, "Blockchain and emerging technologies for next generation secure healthcare: A comprehensive survey of applications, challenges, and future directions," *Blockchain: Research and Applications*, vol. 5, p. 100305 (2024).

[6] A. Andreou, C. X. Mavromoustakis, E. K. Markakis, G. Mastorakis, E. Pallis, and A. Bourdena, "Exploring quantum-resistant cryptography solutions for health data exchange," in *Intelligent Technologies for Healthcare Business Applications*, ser. Signals and Communication Technology, vol. 2032, Cham, Switzerland: Springer Nature, pp. 19–47 (2024), doi: 10.1007/978-3-031-58527-2_2.

[7] N. R. Pradhan, S. S. Rout, and A. P. Singh, "Blockchain based smart healthcare system for chronic-illness patient monitoring," in *Proc. 3rd Int. Conf. Energy, Power and Environment (ICEPE)*, Shillong, India, pp. 1–6 (2021), doi: 10.1109/ICEPE50861.2021.9404496.

[8] S. Saxena, S. Saxena, and N. Tahilramani, "Blockchain enhanced smart healthcare management for chronic diseases," *Discover Computing*, vol. 28, Art. no. 112 (2025).

[9] S. Purohit, P. Calyam, M. L. Alarcon, N. R. Bhamidipati, A. Mousa, and K. Salah, "HonestChain: Consortium blockchain for protected data sharing in health information systems," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 3012–3028 (2021).

[10] S. Jiang, J. Cao, J. A. McCann, Y. Yang, and X. Wang, "Privacy-preserving and efficient multi-keyword search over encrypted data on block-

chain," in *Proc. 2019 IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, USA, pp. 405–410 (Jul. 2019), doi: 10.1109/Blockchain.2019.00062.

[11] R. Rajamanickam, R. Mishra, and S. Chaturvedi, "Designing a dynamic privacy index for assessing blockchain privacy and security in decentralized systems," *Journal of Integrated Science and Technology*, vol. 14, no. 2, Art. no. 1530 (2026), doi: 10.62110/sciencein.jist.2026.v14.1530.

[12] R. Muth and F. Tschorsch, "SmartDHX: Diffie-Hellman key exchange with smart contracts," in *Proc. IEEE Int. Conf. Decentralized Applications and Infrastructures (DAPPS)*, Paris, France, pp. 164–168 (2020), doi: 10.1109/DAPPS49028.2020.00026.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11743–11757 (2021).

[14] H. Gao, H. Huang, L. Xue, F. Xiao, and Q. Li, "Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for EHR sharing," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18414–18425 (2023).

[15] S. Rani, D. Gupta, N. Herencsar, and G. Srivastava, "Blockchain-enabled cooperative computing strategy for resource sharing in fog networks," *Internet of Things*, vol. 21, Art. no. 100672 (2023), doi: 10.1016/j.iot.2022.100672.

[16] D. Ameyed, F. Jaafar, F. Charette-Migneault, and M. Cheriet, "Blockchain Based Model for Consent Management and Data Transparency Assurance," *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Hainan, China, pp. 1050-1059 (2021), doi: 10.1109/QRS-C55045.2021.00159.

[17] S. Kumari and H. Tewari, "Implementation of privacy-preserving identifiers for the secure storage of electronic health records on the Ethereum blockchain," *Distributed Ledger Technologies*, vol. 5, no. 2, Art. no. 15 (Jun. 2026), doi: 10.1145/3743695.

[18] R. M. Purohit, J. P. Verma, R. Jain, and A. Kumar, "FedBlocks: Federated learning and blockchain-based privacy-preserved pioneering framework for IoT healthcare using IPFS in Web 3.0 era," *Cluster Computing*, vol. 28, no. 2, Art. no. 139 (2025), doi: 10.1007/S10586-024-04738-3.

[19] C. C. Agbo and Q. H. Mahmoud, "Design and Implementation of a Blockchain-Based E-Health Consent Management Frame-

work," *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Toronto, ON, Canada, pp. 812-817 (2020), doi: 10.1109/SMC42975.2020.9283203.

[20] C. Hu, C. Li, G. Zhang, Z. Lei, M. Shah, Y. Zhang, C. Xing, J. Jiang, and R. Bao, "CrowdMed-II: A blockchain-based framework for efficient consent management in health data sharing," *World Wide Web*, vol. 25, no. 3, pp. 1489–1515 (2022).

[21] A. Chaurasia, A. K. Sharma, and S. K. Sharma, "Post quantum cryptography for blockchain security using CRYSTALS-Dilithium authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 8, pp. 3121–3132 (2025), doi: 10.47974/JDMSC-2588.

[22] E. Uslu and O. Yayla, "Dilithium-Based Verifiable Timed Signature Scheme," *2024 17th International Conference on Security of Information and Networks (SIN)*, Sydney, Australia, pp. 1-8 (2024), doi: 10.1109/SIN63213.2024.10871762.

[23] A. Haddad, M. H. Habaebi, F. E. M. Suliman, E. A. A. Elsheikh, M. R. Islam, and S. A. Zabidi, "Generic patient-centered blockchain-based EHR management system," *Applied Sciences,* vol. 13, no. 3, Art. no. 1761 (2023).

[24] S. Rai, A. K. Upadhyay, D. Sharma, D. Raj, A. K. Gupta, and D. Ather, "Quantum cryptography—A modern approach," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 7, pp. 1991–2006 (2023), doi: 10.47974/JDMSC-1839.

[25] G. M. Upadhyay, R. Priya, M. Joshi, M. Narula, P. Vats, and P. K. Soni, "Data security challenges and its solutions in cloud computing through quantum resistant advanced encryption standards," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 4, pp. 1151–1160 (2024), doi: 10.47974/JDMSC-1970.

[26] B. Saini, V. K. Verma, P. K. Tiwari, and M. V. C. Varma, "Quantum Digital Signatures (QDS): A novel approach to safeguarding electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 5, pp. 1613–1622 (2023), doi: 10.47974/JDMSC-1837.

[27] R. Mishra, I. Kaur, S. Sahu, S. Saxena, N. Malsa, and M. Narwaria, "Establishing three layer architecture to improve interoperability in Medicare using smart and strategic API led integration," *SoftwareX,* vol. 22, p. 101376 (2023), doi: 10.1016/j.softx.2023.101376.

Received November, 2025