International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 14, No. 1, April 2025, pp. 59~67
ISSN: 2252-8776, DOI: 10.11591/ijict.v14i1.pp59-67

Efficient blockchain based solution for secure medical record management

Debani Prasad Mishra[1], B Rajeev[1], Soubhagya Ranjan Mallick[2], Rakesh Kumar Lenka[3], Surender Reddy Salkuti[4]
[1]Department of Electrical and Electronics Engineering, IIIT Bhubaneswar, Odisha, India
[2]School of Technology, Woxsen University, Hyderabad, Telangana, India
[3]Department of Computer Science, Central University of Odisha, Odisha, India
[4]Department of Railroad and Electrical Engineering, Woosong University, Daejeon, Republic of Korea

Article Info

Article history:

Received Jul 6, 2024
Revised Oct 6, 2024
Accepted Oct 19, 2024

Keywords:

Blockchain
Healthcare
IPFS
Privacy
Scalability

ABSTRACT

Electronic medical records (EMRs) have become a key player in the healthcare ecosystem contributing to the assessment of ailments, the choice of the treatment avenue, and the delivery of services. However, there is consideration of EMR storage whereby centralized storage leads to increased security and privacy issues in the patient's record. In this paper, we proposed a blockchain and interplanetary file system (IPFS) based prototype model for EMR management. It provides a smart contract-enabled decentralized storage platform where healthcare data security, availability, and access management are prioritized. This model also employs cryptographic techniques to protect sensitive healthcare data. Finally, the model is evaluated in a realistic scenario. The experimental results demonstrate that compared to the current systems, the proposed prototype model outperforms them in terms of efficiency, privacy, and security.

Corresponding Author:

Surender Reddy Salkuti
Department of Railroad and Electrical Engineering, Woosong University
17-2, Jayang-Dong, Dong-Gu, Daejeon - 34606, Republic of Korea
Email: surender@wsu.ac.kr

1. INTRODUCTION

The use of electronic medical records (EMRs) has become a popular tool in the provision of health care. EMRs enhance patients' care through the sharing of comprehensive details of the patient across care providers improving diagnosis, treatment planning, and continuity of care. However, having EMRs stored centrally in the traditional healthcare systems is a security and privacy issue. Data breaches can leak sensitive patient information, leading to identity theft, financial fraud, and reputational damage [1]–[3]. Also, the centralized systems do not show the patient the details of who has accessed their records and for what reason or purpose [4], [5]. Blockchain technology has emerged as a potential solution to address these challenges. Blockchain is a distributed and decentralized system of recording and verifying transactions on a network of computers rather than a centralized control system [6], [7]. Every transaction is digitally signed and connected sequentially with the previous post-transaction; this makes it practically hard for anyone to manipulate the records [8]. It is mainly for this reason that data incorporated within a blockchain is almost impossible to alter or manipulate in any way [9]. Various research papers reported the use of blockchain technology as a platform for safe and authorized EMR storage and retrieval. Currently, most healthcare systems administrators have incorporated Blockchain as a core technology that assists with patient-centric care [10].

Blockchain-based healthcare systems provide users more control over their healthcare data, which fosters personal data management and sharing as and when healthcare providers need it. Centralized failure is completely eliminated in blockchain-based healthcare systems. Without any human interaction, a predefined and self- executable smart contract handles device registration, verification, and access control of the healthcare system [11], [12]. It also keeps track of the user's activity on the platform. Most modern healthcare systems face several issues, including security, privacy, efficiency, and scalability, due to the rapid increase in both the number of patients and the volume of healthcare data [13]. The processing overhead of blockchain networks is increasing with the amount of healthcare data, lowering both system efficiency and the rate of patient treatment. An interplanetary file system (IPFS) is incorporated with a blockchain, which stores data in a distributed and decentralized platform to reduce the processing overhead on the blockchain network and make the healthcare system more scalable and secure [14], [15]. In the IPFS storage system, the healthcare data are divided into chunks and stored in a distributed manner, which are cryptographically linked with the hash values [16].

2. LITERATURE REVIEW

Kumar and Chand [17] proposed a Hyperledger Fabric-based MedHypChain medical data exchange system that leverages Identity-based broadcast group encryption to secure transactions, assuring confidentiality, anonymity, traceability, and unforgeability. It secures authenticity, scalability, and access control, which only authorized users can access. Verma [18] present a blockchain-enabled cloud system for health data security using improved Blowfish encryption. Elephant herding optimisation with opposition-based Learning (EHO-OBL) key generation improves this proposed system's data integrity and authenticity. With a 10 KB file size, the proposed method reduces key generation time by 92.64% compared to RivestShamir-Adleman (RSA), Blowfish, elliptic-curve cryptography (ECC), advanced encryption standard (AES), elephant herding optimization (EHO), moth-flame optimization (MFO), and whale optimization (WOA) models. An IPFS and permission Blockchain-enabled healthcare data-sharing system using Hyperledger Besu's Istanbul byzantine fault tolerance (IBFT) consensus algorithm and threshold signatures is proposed by Shuaib *et al.* [19]. It gives better results than existing Blockchain healthcare systems in transaction throughput, latency, and failure rate. Zakzouk *et al.* [20] proposed a blockchain-based EMR management framework for a smart city healthcare system that prioritizes patient record security, privacy, and ownership. Scalability is achieved by off-chain storage while preserving the authenticity of medical records. Mallick *et al.* [21] proposed a fog node computing-based IoMT and Blockchain architecture to reduce latency, congestion, and overload. A proxy monitor connects untrusted devices, and IPFS integration provides decentralized, scalable, secure, and private data storage. A secure IoMT-based data-collection approach proposed by Dewangan and Chandrakar [22] that maintains patient data on the blockchain ensures GDPR compliance. Data is sent to the cloud through the patient's PDA IoMT devices, where a miner selection process prevents blockchain bias. The system's resiliency was verified using Scyther security protocol analysis and Bevywise internet of things (IoT) and message queuing telemetry transport (MQTT) simulator assaults. A blockchain-based access control model (BBACM) was introduced by Masood *et al.* [23] to improve patient data privacy and security in S-CI. In a paralysis patient use case, authorization rights for patient physiological parameters (PPPs) and PHI are successfully maintained by BBACM. Blockchain's decentralization and immutability properties enhance PHI access control, security, scalability, Privacy, and availability of healthcare systems. Uppal *et al.* [24] proposed a healthcare system that uses IoT devices, IPFS, and blockchain to upload and monitor health data for clinicians and insurance companies. It uses DoteCoins to trade consultations, medications, insurance payments, and medical supplies across six blockchains. Additionally, it provides emergency alerts and lifestyle notifications. Abdelgalil and Mejri [25] proposed the HealthBlock framework, which integrates technologies to enable EHR collaboration and privacy. It provides patients full ownership over their EHRs, while Fabric handles patient access control policies and delegations. IPFS stores and shares EHRs off-chain, assuring immutability. A consortium blockchain-based EMR sharing method using IPFS was proposed by Liu *et al.* [26]. It employs attribute-based access control, a proxy re-encryption algorithm for user authentication, and data privacy. To optimize energy consumption and enhance data quality in IoT-based healthcare, a secure data fusion-based data aggregation technique was proposed by Singh and Kumar [27]. Better connectivity and sensor selection are improved using the archimedes optimisation algorithm (AOA) and extended belief propagation.

3. PROPOSED PROTOTYPE MODEL

Figure 1 shows the proposed prototype model which ensures the EMR storage and control of data using Blockchain technology. The framework harnesses cryptographic mechanisms and smart contracts to provide data tamper-proofing, access control at a granular level, and transparency. This section provides a clear overview of the execution of the proposed model.

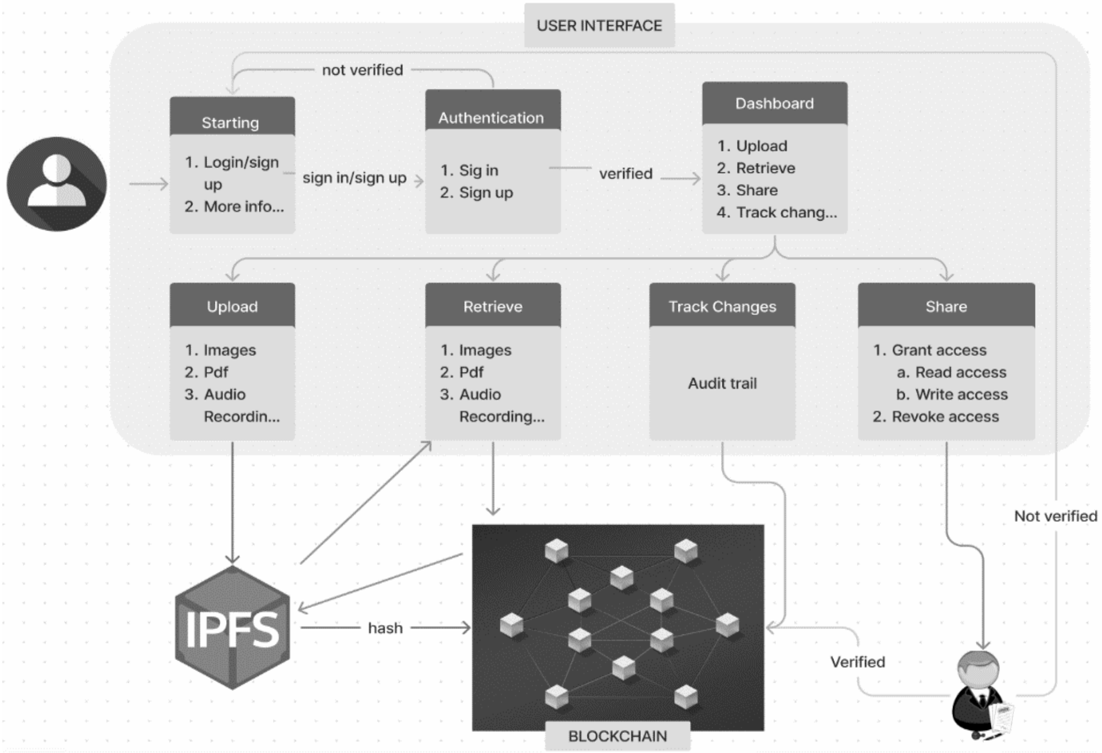


Figure 1. Key components of the system

3.1. Data encryption

The EMRs are encrypted to ensure that the data is secure before being uploaded to the IPFS. This ensures that unauthorized individuals do not get access to sensitive medical data. The encryption process employs the use of the public key/ private key security system whereby the patient possesses the private key for decryption while the public key is for encryption [28].

3.2. Smart contracts

They are self-executing programs that run on the blockchain network. These contracts in actuality provide the terms governing exactly who gets to use the patient’s EMRs and in what circumstances. The access control policy can be dependent on factors such as the role and specialty of the HCP or even the information that has been requested [29].

3.3. Access control process

The process of access control is as follows: (i) Request for access: when ever an HCP requires the patient’s EMR, then the HCP puts in a request to the blockchain network. This request comprises the identification of HCP and the details of the data they need. (ii) Policy evaluation: access control implemented for each EMR is based on a smart contract and when the patient attempts to access information, the request is compared to the access control policy. (iii) Grant/deny access: if the policy allows the requested data, the smart contract allows access as per the request. Otherwise, access is denied.

3.4. Auditability

It should also be noted, that the proposed framework has high auditability. Any access attempt made toward patient EMR is stored permanently in the blockchain database to facilitate a clear trail of who accessed the data, when, or why. These access logs may be checked by auditors to detect any undesirable tendencies, or attempts at illegitimate access. Moreover, the restricted alteration of the blockchain indicates that the access control policies can never be changed, which, in turn, makes it a highly auditable system [30].

3.5. Implementation considerations

Several issues and concerns that need to be taken into consideration when implementing the proposed framework for EMR management include:

- Scalability: one of the main weaknesses associated with public blockchain solutions like Ethereum is that a large number of transactions can slow down the process and increase the time for its completion. There is an expectation that permissioned blockchains [31], [32] can be a solution to both issues, however, they involve a third party to decide who can be a participant.
- Interoperability: different blockchain platforms may have varying protocols and data structures. Ensuring interoperability between different blockchain-based EMR systems is crucial for seamless data exchange in the healthcare ecosystem. Standardized protocols and data formats are needed to facilitate interoperability.

Figure 1 explains how these components are related to one another. The system comprises four main actors: self-owners: (i) Patients: legal entities to whom certain medical data belongs to and who grant/deny access. (ii) Healthcare providers (HCPs): healthcare workers who are legally permitted to see and amend patient EMRs based on their role. (iii) Blockchain network: a distributed ledger that stores encrypted EMR data and access control policies [33]. (iv) IPFS: is a decentralized storage system where all files including all images will be stored.

A user in the network can upload a file based on the content address of the file. Other peers in the network are also allowed to look up and subsequently request certain content from any node in the network using a distributed hash table (DHT). Figure 2 shows the access control mechanism discussed above and the sequence of operations that will take place in this decentralized medical storage platform.

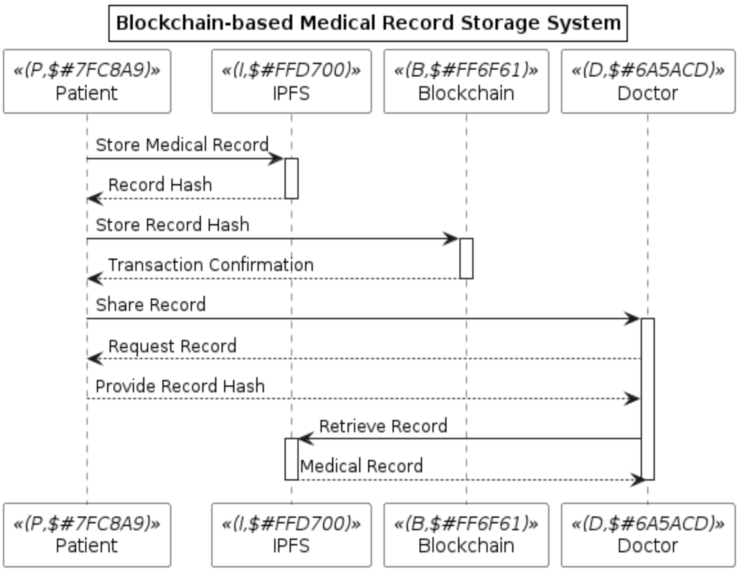


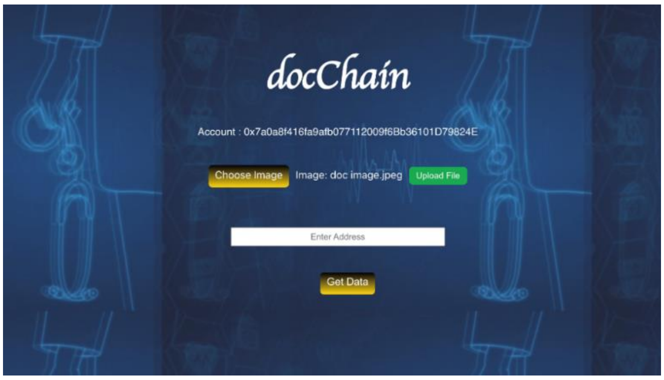
Figure 2. Sequence diagram

4. RESULTS AND DISCUSSION

This paper presents a practical implementation of a blockchain-based medical record storage system. Currently, the smart contract is deployed on the Ethereum Sepolia test net and the images are stored in the IPFS. After uploading a document in the IPFS, a hash is generated, and this hash is stored in the blockchain. Storing the entire image or document in the blockchain would be expensive, so the first images are stored in IPFS, and their hash is stored in the blockchain. The source code is provided in the GitHub link along with the working project link [34]. To open the application, MetaMask must be installed in the browser and the remaining requirements are mentioned in the GitHub readme page. The front end is hosted on Netlify, but to improve its security even further, it can also be hosted on the Internet computer blockchain.

4.1. User interface analysis

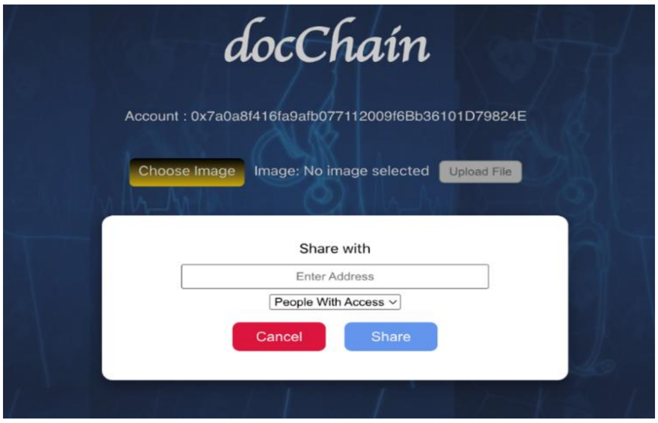
Figure 3 shows the first page of the application, and it has the option to choose the document, upload it, and share it with the health care provider. To share the access of the document with others, we must enter the MetaMask account hash and then select the share option. Figure 4 shows the interface to share the EMR with healthcare providers. The “People with access” option shows the list of all accounts that have access to the current document.



Account : 0x7a0a8f416fa9afb077112009f6Bb36101D79824E

Image: doc image.jpeg

Figure 3. User interface of the blockchain based EMR management system



Account : 0x7a0a8f416fa9afb077112009f6Bb36101D79824E

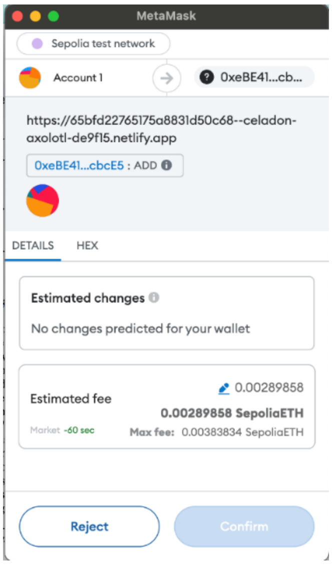
Image: No image selected

Figure 4. Sharing EMR access with healthcare providers

4.2. Enhanced security

The present blockchain-based framework introduced in this study is superior in the security of EMRs over the conventional centralized systems. Due to the unalterable feature of blockchain, every block holding information on the executed transactions cannot be tampered with. If one wanted to change the data contained in the block then they would have to change data in all subsequent blocks which due to the distributed nature of the blockchain would be mathematically impossible. What is more important is the fact that it ensures that there are no changes to the data that have already been saved and stored since it is immutable. Figures 5 and 6 show the MetaMask transaction process and its confirmation status respectively. Each transaction on the blockchain involves some gas fees. We can see the total transaction fees required for the upload function in the Sepolia testnet of the Ethereum blockchain.

The use of blockchain keeps a record of all the access attempts made on the patient EMRs, as well as ensuring that the records are transparent and difficult to alter. This high level of auditability has the advantage of increasing accountability in the system and the integrity of the healthcare data. Despite the various strengths of the framework regarding security, the aspect of scalability could be a problem with the system. Centralised blockchains such as Ethereum can get crowded when there are many transactions and this results to increased processing time as well as increased transaction fees. Permissioned blockchains could be a potential solution to this but they involve the usage of a control system to regulate the participants hence taking some of the decentralization advantages away. Table 1 shows the actual transaction fees for each operation like adding the image hash to the blockchain along with their block number and transaction hash. We can see from the table that the gas fees vary from time to time and with the network traffic.


MetaMask

Sepolia test network

Account 1 → 0xeBE41...cb...

https://65bfd22765175a8831d50c68--celadon-axolotl-de9f15.netlify.app

0xeBE41...cbcE5 : ADD

DETAILS HEX

Estimated changes

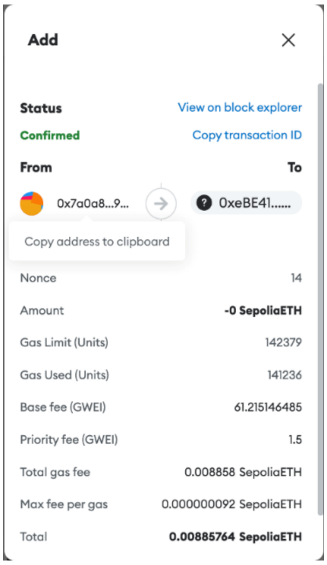
No changes predicted for your wallet

Estimated fee 0.00289858

0.00289858 SepoliaETH

Market -60 sec Max fee: 0.00383834 SepoliaETH

Reject Confirm


Add

Status View on block explorer

Confirmed Copy transaction ID

From To

0x7a0a8...9... → 0xeBE41......

Copy address to clipboard

Nonce 14

Amount -0 SepoliaETH

Gas Limit (Units) 142379

Gas Used (Units) 141236

Base fee (GWEI) 61.215146485

Priority fee (GWEI) 1.5

Total gas fee 0.008858 SepoliaETH

Max fee per gas 0.000000092 SepoliaETH

Total 0.00885764 SepoliaETH

Figure 5. Confirming the transactions in MetaMask Figure 6. Transaction confirmed status in MetaMask

Table 1. Simulation results

S. No	Method	Block no.	Txn fees (In ethers)	Transaction hash
1	Add	6030041	0.0088576	0x2e5e1dbe31f8d67e772e2d053a02eb26bad736e40fc989e431d463e6d91dca08
2	Add	5694043	0.0002118	0x6cbc4937ec6cc4a8d0fb3921b136e05f3c713e297c2eed86c483f5ff0470816f
3	Transfer	5279469	0.001155	0x720f3ac8cc6f872fe9a2b91a78deab62c703bf93dad46b1db340863c9818e433
4	Transfer	5218137	0.0001423	0x51d93b1a4264b5d2c6934759ff4e99a53f91ba4e72daef0c3436fa3d4c1263eb
5	Add	521814	0.0008735	0x06d2c191c41d85991f525dc9b0db3d3881986644a298f6190ecb4f049dbe0b38
6	Add	523768	0.0039857	0xc51b035dc65275febe0f66a24f842f467f0ebeeea493d90999edb82a847f4e9e
7	Add	5219574	0.00093949 0.00093949	0xe051043bb406f976d29603d59748667cec18b9370d8fb2d647aac4f3abc49b9f

4.3. Interoperability and standards

The ability to share data between various blockchain-based EMR systems will require integration to enhance data sharing within the healthcare system. These blockchains can be very dissimilar in terms of devices, syntactic structures, semantics, protocols, and even programming paradigms, which can reduce the ease of interconnectivity. Table 2 compares 4 famous blockchains based on various parameters. This comparison allows users to suitably choose the blockchain of their choice.

Table 2. Comparison of blockchain frameworks in healthcare data management

S. No	Feature	Hyperledger Fabric	Ethereum	Corda	Quorum
1	Consensus mechanism	BFT (Practical byzantine fault tolerance)	Proof of stake	Notary (Unique consensus per transaction)	IBFT (Istanbul byzantine fault tolerance)
2	Privacy and confidentiality	High-channels and private data	Moderate-public and private options	High-Focus on privacy	High-private transactions
3	Smart contract language	Go, Java, Node.js	Solidity	Java, Kotlin	Solidity
4	Transaction speed	1,000-3,000 TPS	15-30 TPS (PoW), 1,000+ TPS (PoS)	170 TPS	2,000+ TPS
5	Governance model	Permissioned	Public/Permissioned	Permissioned	Permissioned
6	Use case suitability	Supply chain, Finance, Healthcare	ICOs, DApps, Healthcare	Finance, trade finance	Financial services, Healthcare
	Data immutability	High	High	Moderate	High
7	Interoperability	Moderate	High	Moderate	High

The studies established that the proposed blockchain-based framework for EMR management significantly improved the system's security, privacy, and transparency. Cryptographic techniques and smart contracts make data immutable and provide the privilege of fine-grained access control to avoid the drawbacks of centralized systems.

5. CONCLUSIONS

This paper has discussed the framework for secure storage and proper application of EMRs through the use of blockchain technology. The given framework employs cryptographic approaches and smart contracts to achieve the data's tamper-proofness; permissioned access; and traceability. The introduced approach is considerably more secure, private, and transparent than a conventional centralized EMR system. Despite the known issues of blockchain in terms of scalability or interoperability and legal issues that are still critical, the constant innovations and experiments are helping in integrating blockchain in the health data management domain. Further studies should investigate achieving scalability of the blockchain networks, working for harmonization of interface standards between the participants and case-study-based validation of the given framework in the healthcare context. Addressing these research directions stated above, blockchain can boost EMR management to change the nature of the healthcare system toward a more secure, private and transparent one.

ACKNOWLEDGEMENTS

This research work was supported by "Woosong University's Academic Research Funding - 2025".

REFERENCES

[1] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Information Sciences*, vol. 629, pp. 703–718, Jun. 2023, doi: 10.1016/j.ins.2023.01.148.

[2] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: a secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, Dec. 2021, doi: 10.1016/j.comnet.2021.108500.

[3] S. R. Mallick *et al.*, "BCGeo: blockchain-assisted geospatial web service for smart healthcare system," *IEEE Access*, vol. 11, pp. 58610–58623, 2023, doi: 10.1109/ACCESS.2023.3283776.

[4] M. A. Mohammed *et al.*, "Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology," *Engineering Applications of Artificial Intelligence*, vol. 129, p. 107612, Mar. 2024, doi: 10.1016/j.engappai.2023.107612.

[5] D. Rani, R. Kumar, and N. Chauhan, " A secure framework for IoT -based healthcare using blockchain and IPFS ," *Security and Privacy*, vol. 7, no. 2, Mar. 2024, doi: 10.1002/spy2.348.

[6] A. Adimabua Ojugo, P. O. Ejeh, O. C. Christopher, A. O. Eboka, and F. U. Emordi, "Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 12, no. 3, p. 205, Dec. 2023, doi: 10.11591/ijict.v12i3.pp205-213.

[7] U. Mishra, R. Gupta, and J. Gupta, "InterPlanetary file system based blockchain for internet of medical things," *International Journal of Information Technology*, vol. 15, no. 4, pp. 1769–1776, Apr. 2023, doi: 10.1007/s41870-023-01207-9.

[8] R. Kumar and R. Tripathi, "Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 7916–7955, Aug. 2021, doi: 10.1007/s11227-020-03570-x.

[9] S. R. Mallick, S. Sharma, P. K. Tripathy, and N. K. Ray, "Adoption of Blockchain-Fog-IoMT framework in Healthcare 4.0 digital revolution," in *2022 OITS International Conference on Information Technology (OCIT)*, Dec. 2022, pp. 603–608, doi: 10.1109/OCIT56763.2022.00117.

[10] G. Shankar, P. Singh, N. K. Dewangan, and P. Chandrakar, "DEMRISEC: security enhancement of patient data in decentralized medical records with IPFS," *Multimedia Tools and Applications*, pp. 1–18, May 2024, doi: 10.1007/s11042-024-19444-w.

[11] A. Bisht, A. K. Das, D. Niyato, and Y. Park, "Efficient personal-health-records sharing in internet of medical things using searchable symmetric encryption, Blockchain, and IPFS," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2225–2244, 2023, doi: 10.1109/OJCOMS.2023.3316922.

[12] M. Sadeghi and A. Mahmoudi, "Synergy between blockchain technology and internet of medical things in healthcare: a way to sustainable society," *Information Sciences*, vol. 660, p. 120049, Mar. 2024, doi: 10.1016/j.ins.2023.120049.

[13] S. M. Nagarajan, P. Anandhan, V. Muthukumaran, K. Uma, and U. Kumaran, "Security framework for IoT and deep belief network-based healthcare system using blockchain technology," *International Journal of Electronic Business*, vol. 17, no. 3, p. 226, 2022, doi: 10.1504/IJEB.2022.124324.

[14] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, p. 1110, Jun. 2022, doi: 10.3390/healthcare10061110.

[15] S. R. Mallick, V. Goswami, R. K. Lenka, T. R. Sahoo, V. Kumar, and R. K. Barik, "Blockchain-based IoMT for an intelligent healthcare system using a drop-offs queue," in *2023 First International Conference on Microwave, Antenna and Communication (MAC)*, Mar. 2023, pp. 1–6, doi: 10.1109/MAC58191.2023.10176337.

[16] T. L. Quy *et al.*, "Blockchain-driven animal healthcare: leveraging NFTs, IPFS, and smart contracts for comprehensive animal medical record," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 14482 LNCS, 2024, pp. 100–119.

[17] M. Kumar and S. Chand, "MedHypChain: a patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic," *Journal of Network and Computer Applications*, vol. 179, p. 102975, Apr. 2021, doi: 10.1016/j.jnca.2021.102975.

[18] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *Journal of Experimental and Theoretical Artificial Intelligence*, vol. 36, no. 1, pp. 147–160, Jan. 2022, doi: 10.1080/0952813X.2022.2135611.

[19] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, “Secure decentralized electronic health records sharing system based on blockchains,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5045–5058, 2022, doi: 10.1016/j.jksuci.2021.05.002.

[20] A. Zakzouk, A. El-Sayed, and E. E.-D. Hemdan, “A blockchain-based electronic medical records management framework in smart healthcare infrastructure,” *Multimedia Tools and Applications*, vol. 82, no. 23, pp. 35419–35437, Sep. 2023, doi: 10.1007/s11042-023-15152-z.

[21] S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, “A lightweight, secure, and scalable blockchain-fog-IoMT healthcare framework with IPFS data storage for healthcare 4.0,” *SN Computer Science*, vol. 5, no. 1, p. 198, Jan. 2024, doi: 10.1007/s42979-023-02511-8.

[22] N. K. Dewangan and P. Chandrakar, “Patient-centric token-based healthcare blockchain implementation using secure internet of medical things,” *IEEE Transactions on Computational Social Systems*, vol. 10, no. 6, pp. 3109–3119, Dec. 2023, doi: 10.1109/TCSS.2022.3194872.

[23] I. Masood, A. Daud, Y. Wang, A. Banjar, and R. Alharbey, “A blockchain-based system for patient data privacy and security,” *Multimedia Tools and Applications*, vol. 83, no. 21, pp. 60443–60467, Jan. 2024, doi: 10.1007/s11042-023-17941-y.

[24] S. Uppal, B. Kansekar, S. Mini, and D. Tosh, “HealthDote: a blockchain-based model for continuous health monitoring using interplanetary file system,” *Healthcare Analytics*, vol. 3, p. 100175, Nov. 2023, doi: 10.1016/j.health.2023.100175.

[25] L. Abdelgalil and M. Mejri, “HealthBlock: a framework for a collaborative sharing of electronic health records based on blockchain,” *Future Internet*, vol. 15, no. 3, p. 87, Feb. 2023, doi: 10.3390/fi15030087.

[26] G. Liu, H. Xie, W. Wang, and H. Huang, “A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption,” *Journal of Cloud Computing*, vol. 13, no. 1, p. 44, 2024, doi: 10.1186/s13677-024-00608-w.

[27] S. Singh and D. Kumar, “Energy-efficient secure data fusion scheme for IoT based healthcare system,” *Future Generation Computer Systems*, vol. 143, pp. 15–29, Jun. 2023, doi: 10.1016/j.future.2022.12.040.

[28] P. P. Ray, “A survey on internet of things architectures,” *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[29] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, and C.-C. Lee, “A blockchain based data aggregation and group authentication scheme for electronic medical system,” *IEEE Access*, vol. 8, pp. 173904–173917, 2020, doi: 10.1109/ACCESS.2020.3025898.

[30] R. Mishra, D. Ramesh, D. R. Edla, and L. Qi, “DS-Chain: a secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain,” *Journal of Industrial Information Integration*, vol. 26, p. 100315, Mar. 2022, doi: 10.1016/j.jii.2021.100315.

[31] S. R. Salkuti, “Emerging and advanced green energy technologies for sustainable and resilient future grid,” *Energies*, vol. 15, no. 18, p. 6667, Sep. 2022, doi: 10.3390/en15186667.

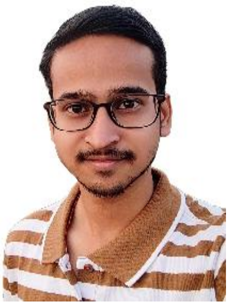
[32] D. Jhunjhunwalla, D. P. Mishra, D. Hembram, and S. R. Salkuti, “Revolutionizing domestic solar power systems with IoT-enabled Blockchain technology,” *International Journal of Applied Power Engineering (IJAPE)*, vol. 13, no. 1, p. 255, Mar. 2024, doi: 10.11591/ijape.v13.i1.pp255-262.

[33] P. Meghana, C. Yammani, and S. R. Salkuti, “Blockchain technology based decentralized energy management in multi-microgrids including electric vehicles,” *Journal of Intelligent & Fuzzy Systems*, vol. 42, no. 2, pp. 991–1002, Jan. 2022, doi: 10.3233/JIFS-189766.

[34] B. Rajeev, Feb 4. 2024, "DocChain,". [Online]. Available: https://github.com/rajeev82604/DocChain.

BIOGRAPHIES OF AUTHORS

Debani Prasad Mishra is working as assistant professor in Electrical Engineering Department in International Institute of Information Technology, Bhubaneswar, Odisha. He completed his B.Tech. in Electrical Engineering from the Biju Patnaik University of Technology, Odisha, India in the year 2006. He then did his M.Tech. in Power Systems from IIT Delhi, India, in 2010 and subsequently earned his Ph.D. in Power Systems from Veer Surendra Sai University of Technology, Odisha, India, in 2019. His research interests are in the fields of soft computing in signal processing, power quality, and power systems. He can be contacted at email: debani@iiit-bh.ac.in.



B Rajeev is a student in the Electrical and Electronics Engineering department at the International Institute of Information Technology, Bhubaneswar. His research interests encompass Blockchain technology and Web development, areas in which he actively engages through both academic and personal projects. Rajeev’s expertise extends to Data Structures and Algorithms, fundamental components that underpin his ability to solve complex problems and enhance the efficiency of his implementations. His proficiency in these areas significantly contributes to his capability to address intricate computational challenges and optimize system performance. He can be contacted at email: b322014@iiit-bh.ac.in.

Soubhagya Ranjan Mallick is pursuing his Ph.D. Computer Science and Engineering degree at IIIT Bhubaneswar, Odisha, India. He works as an assistant professor in the School of Technology, Woxsen University, Hyderabad, Telangana, India. He has more than 13 years of experience in teaching and research. His research interests include IoT, blockchain, cryptography, edge computing, fog computing, and cloud computing. He can be contacted at email: soubhagya.mallick@gmail.com.

Rakesh Kumar Lenka is working as an associate professor in the Department of Computer Science, Central University of Odisha. He has published over 60 research articles in reputed journals and conference proceedings. His research interests include green IoT, fog/mist computing, model checking, blockchain technology, recommendation systems, geographical information systems, and DFA-based pattern matching. He is a professional member of the CSI and the International Association of Engineers (IAENG). He has served as a reviewer for various reputed international journals and conferences. He can be contacted at email: rklenka@cuo.ac.in.

Surender Reddy Salkuti received the Ph.D. degree in electrical engineering from the Indian Institute of Technology, New Delhi, India, in 2013. He was a Postdoctoral Researcher with Howard University, Washington, DC, USA, from 2013 to 2014. He is currently an associate professor with the Department of Railroad and Electrical Engineering, Woosong University, Daejeon, South Korea. His current research interests include market clearing, including renewable energy sources, demand response, smart grid development with integration of wind and solar photovoltaic energy sources. He can be contacted at email: surender@wsu.ac.kr.