International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Enhancing the Security and Privacy of eHealth Records through Blockchain-based Management: A Comprehensive Framework

[1]Abida Khanam, [2]Mohd Faizan Farooqui
[1]Department of Computer Application
Integral University
Lucknow, India
abidakhan@iul.ac.in
[2]Department of Computer Application
Integral University
Lucknow, India
ffarooqui@iul.ac.in

Abstract— Progress in information technology is transforming the healthcare sector with the goal of enhancing medical services, diagnostics, and continuous monitoring through wearable devices, among other benefits, while also lowering expenses. This digital transformation enhances the convenience of computing, storing, and retrieving medical records, ultimately leading to improved treatment experiences for patients. Electronic health record systems have come under fire for centralized control, faults, and attack points with transferring data custodians. These systems are frequently utilized for the interchange of health information among healthcare stakeholders. The main objective is to overcome information asymmetry and data breaches commonly encountered in the Electronic Health Record (EHR) system. This study introduces a decentralized and trustless architecture aimed at securely storing patients' medical records and granting access to authorized individuals, including healthcare providers and patients themselves. The research primarily focuses on bolstering the security and privacy of healthcare data management systems using blockchain technology. To address the issue of blockchain scalability, an off-chain scaling approach is proposed, utilizing an underlying medium to store large volumes of data. This is achieved through the integration of Elliptic Curve Cryptography (ECC) and the Interplanetary File System (IPFS). The proposed system provides a secure and efficient method for storing and sharing sensitive healthcare data while ensuring confidentiality and data integrity.

Keywords-blockchain; smart contract; IPFS; ECC; EHR.

I. INTRODUCTION

The traditional method of medical record-keeping relies on manual handwritten documents, which brings several drawbacks, including disorganized chronological information, insufficient data, vulnerable records, data redundancy, inconsistency in handwriting, and occasional inefficiencies. Presently, the healthcare industry is witnessing significant transformations worldwide, particularly with the adoption of Electronic Health Record (EHR) systems[1]. These systems efficiently manage critical healthcare activities, ranging from maintaining patient medical records and doctor availability to handling clinical and lab test records.

As electronic records continue to increase in number, they form what is known as "big data," which holds immense potential for various purposes in the healthcare domain. Healthcare is becoming increasingly interconnected, and the data being generated is growing in size and complexity[2]. The healthcare industry is data-intensive, generating, distributing, sorting, and accessing massive amounts of data every second. For instance, the global health data produced in 2013 amounted to approximately 153 exabytes, and by 2020, it is projected to reach around 2314 exabytes[2]. To meet the demands for extensive big data storage, various stakeholders have invested in cloud computing and storage solutions. This cloud storage has attracted the interest of patients, healthcare sectors, and research institutions for storing data in secure repositories, facilitating controlled, cross-domain, and flexible data sharing among beneficiaries. However, in the current approach, the centralized cloud is used to store health records. Companies like Amazon, Microsoft, etc., maintain large servers for this purpose. However, this centralized model comes with risks, including a single point of failure and the potential exposure of sensitive data to unauthorized third parties.

One of the major challenges in cloud data storage and sharing is the risk of unauthorized access, especially when dealing with sensitive data like electronic health records. Protecting patient health records is of utmost importance, and it is the responsibility of every individual to ensure the security of electronic health records. The central security issue with a centralized cloud model is privacy and data security[3].

Over the years, healthcare systems have implemented firewall protection to safeguard Electronic Health Records (EHRs). In one approach, the firewall acts as an anomaly-based intrusion detection system (IDS) and can be configured as either a packet filtering firewall or a status inspection firewall. Another method proposed in involves encryption to ensure EHR security during the exchange process. This approach, designed by the Health

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Insurance Portability and Accountability Act (HIPAA), aims to secure EHRs when accessed by patients or when Patient Health Information (PHI) is created, received, maintained, or transmitted through mobile devices[4]. Despite the success of these approaches, malicious intruders continue to find ways to bypass these protective measures and gain unauthorized access to EHRs [Secure Architecture for Inter-Healthcare Electronic Health Records Exchange]. A blockchain is a digital record of transactions organized in a chain-like structure, hence the name "blockchain." It consists of individual records, known as blocks, interconnected, and arranged in a sequential manner. Each transaction must be validated by interconnected nodes before being added to the blockchain. The design of the blockchain ensures that data is distributed across multiple nodes, forming a consensus on the exact location of the data. Unlike traditional centralized cloud storage, where data remains in one location, blockchain divides data into smaller chunks and disperses them across the network, providing an additional layer of security. If an unauthorized individual or entity attempts to breach the system, they will only gain access to a fraction of the data rather than the entire files[5].

Blockchain technology is being utilized in the healthcare sector to address security issues effectively. Health information is encrypted, hashed, and then stored in a distributed manner, ensuring its safety across multiple parties. Each record is added to the previous one, creating a continuous chain of records with individual timestamps. The network encrypts and validates all transactions[6]. Notably, the Estonian government has deployed the Keyless Signature Infrastructure blockchain, which can handle a substantial amount of data, scaling up to 1012 items per second. Although the application of blockchain in Electronic Health Records (EHRs) is still in its early stages, its potential to address existing shortcomings and ensure data security and confidentiality, positions it as a leading candidate for adoption in the healthcare industry. Researchers have explored various implementations of blockchain to safeguard personal data. Blockchain technology has transformed data management, providing transparency, immutability, and decentralization[7]. However, the security and confidentiality of data continue to be major issues. This study presents a unique strategy for improving the security and privacy of blockchain-based systems by combining Elliptic Curve Cryptography (ECC) encryption and Interplanetary File System (IPFS) storage. An electronic contract is a documentation that is held in centralized as well as decentralized data centers that contains data which has been agreed between parties, such as assets and agreements. Decentralized contract storage problems can be handled via IPFS and web-based services. An API with a RESTful connectivity link allows a smart contract, which is the core component of the Ethereum blockchain platform, to interface with IPFS and these other services. For decentralized systems, reducing the quantity of references to the distributed ledger network is crucial. This paper aims to move agreements to an IPFS with blockchain together in a single request. We decide to integrate blockchain technology with IPFS to create an effective, unchangeable system. Stated differently, after publishing information to IPFS, linked participants to the system should transmit one contract to the blockchain rather than several individual requests.

II. PRILIMINARIES

A. Blockchain

Blockchain is a peer-to-peer shared database that keeps track of a list of records that are continually added to and connected chronologically by units of data called blocks. It is protected via public key encryption and hashing techniques. Instead of adding to the centralized database as in a typical centralized system, blockchain technology allows for the addition of new data to a block, which is then made accessible to all peers in a distributed network [8]. Traditionally, a new block is produced to store each new set of transactions that are uploaded to the blockchain network. This new block then becomes a subsequent block in the chain, hence the term "Blockchain."

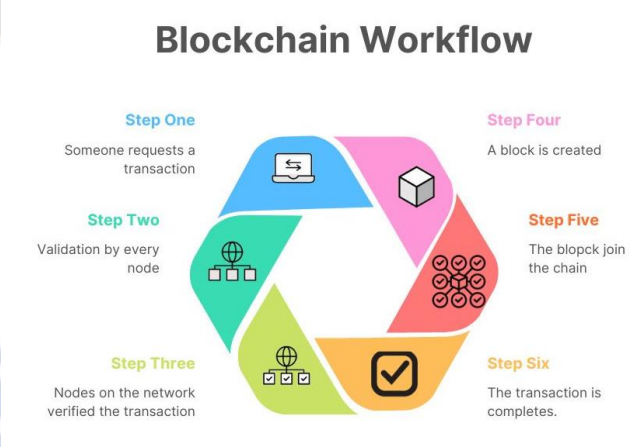

Figure 1. The workflow of blockchain.

According to the 2018 PwC global blockchain report, the financial services sector is now utilizing the most cutting-edge blockchain technology under development. Along with government organizations, healthcare, industrial production, financial services, and media, the entertainment and media industries are also making inroads into the blockchain. The figure (2) shows Statistics on the industries that are most advanced in using blockchain for development.

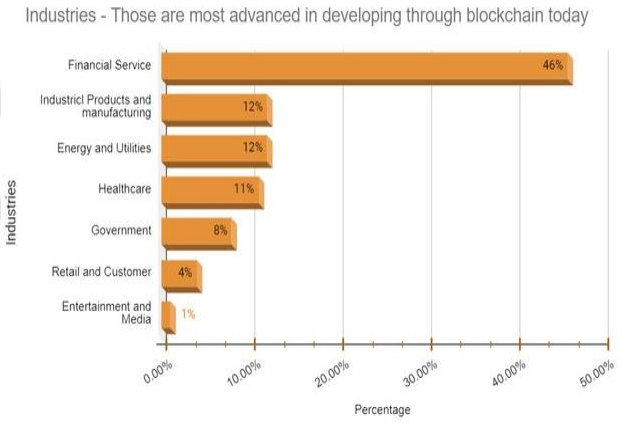

Figure 2. Statistics on the industries that are most advanced in using blockchain to develop [9].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

B. IPFS

The Interplanetary File System (IPFS), a peer-to-peer distributed file system, is another intriguing concept in addition to blockchain. It offers a content-based block-storing model and incorporates a number of previously successful solutions. One of the most popular file-distributed systems today, HTTP, can be improved using IPFS. The IPFS content is duplicate-free. Due to the fact that their hash would provide the same CID, storing identical 1 MB of data in a single IPFS node would result in their storage being done only once, eliminating duplication [10]. Decentralization indicates that the system is not governed by a single entity. By using cryptographic technologies to link the transaction outcomes together, trackability and incorruptibility show that the outcomes on the chain are unassailable.

The Architecture of IPFS:

An architectural framework and collection of fundamental elements provide IPFS the ability to offer a decentralized and content-addressable storage system. Here is a thorough explanation of its architecture:

a) Content-Addressed Data:

• Content Addressing: A key notion in IPFS is content addressing. In IPFS, information is addressed based on its content rather than its domain name or location. A cryptographic hash, which is created from the content of every bit of data, be it a file, a website, or another digital entity, serves as a unique identifier.

• Content Integrity: Any modification to the content leads to an alternate cryptographic hash due to content addressing. The reliability of the data is ensured by this feature. It is very hard to alter IPFS data since even little changes result in a completely new address.

b) Distributed Hash Tables (DHTs):

• Peer Discovery: IPFS makes use of Distributed Hash Tables to speed up the network-wide identification of peers with data. A decentralized for sorting and searching information is called a DHT. A user queries the DHT to identify peers that could have a certain piece of information when they need to find it.

• Peer-to-Peer Network: IPFS is supported by a huge network of linked peers. Each connected peer oversees hosting and disseminating data and running IPFS software. The DHT encourages a peer-to-peer design by enabling users to locate peers who hold the needed data.

c) MerkleDAG Data Structure:

• Data Representation: A MerkleDAG information structure is used in IPFS for encoding files. Each node in a MerkleDAG tree-like structure has a label that includes the encrypted hash of its contents and any child nodes.

• Efficient Distribution: Using the MerkleDAG structure, data may be distributed effectively. After data is broken up into blocks, every block's encrypted hash is calculated and connected to its parents in a tree called Merkle. This structure guarantees that even minor changes to the data cause changes to several nodes within the tree, making it possible to efficiently verify the accuracy of the data.

• Version Control: Data version management is made possible via the MerkleDAG structure. Users can quickly find and access any earlier version of a file by representing various versions as distinct branching in the Merkle tree.

• Addressing: By representing the complete information as the tree's rooted hash, the MerkleDAG structure enables content addresses.

d) MerkleDAG Data Structure:

• Efficient Data Retrieval: To improve the efficiency of data extraction, IPFS stores data locally. Content may be temporarily cached on the user's gadget upon access, eliminating the need for subsequent downloads.

• Reduced Network Traffic: Locally cached data, particularly with regard to frequently requested material, reduces network traffic and speeds up content retrieving.

• Offline Access: Data is kept available regardless of whether the gadget is offline thanks to the local cache. Content that has already been seen by users can be retrieved without a current connection to the internet.

C. Elliptic Curve Cryptography

ECC is an asymmetric encryption technique that uses the algebraic structure of elliptic curves having finite fields, as its name suggests. Elliptic Curve Cryptography is a type of encryption method that supports public-key encryption and is analogous to RSA. While RSA's security is reliant on enormous prime numbers, ECC uses the elliptic curves concept of mathematics to provide the same degree of security with much smaller keys [11]. Fig (3) shows the comparison of the key length of RSA with the ECC technique. It typically has a length of 256 bits (a 256-bit ECC key is comparable to a 3072-bit RSA key), which makes it more secure and able to provide more potent anti-attack capabilities. Furthermore, ECC delivers superior efficiency and uses fewer server resources because its computation is faster than RSA's.

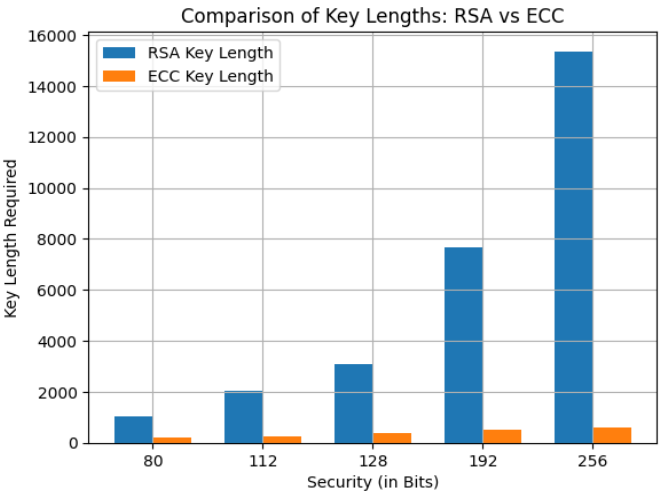

Figure 3. Comparison of key lengths between RSA and ECC Encryption.

In 1985, Victor Miller and Neal Koblitz both independently devised elliptic curve ciphers. On a broad scale, they are analogs of real public cryptosystems, where elliptic curve operations replace modular arithmetic[12]. The well-known NP-Hard Elliptic Curve Discrete Logarithmic Problem is the basis for the ECC. The equation (1) describes an elliptic curve[11].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

$$y^2 = x^3 + ax + b \quad (1)$$

ECC only supported the encryption and decryption of points; hence, the first step (known as encoding) consists of converting a plain text message (t) into a point A(x,y) on the curve to produce At. This is then followed by the encryption process to produce a cipher point (Ct). By first acquiring the plain point At and then decoding the point at to retrieve the plaintext content t, the cipher point Ct may be decrypted.

III. Literature Review

Paper name and publication	Paper Objective	Advantage	Limitation
MedChain, *Springer Nature (2021)* [13]	Blockchain-based medical record management	Ensured data integrity and immutability of medical records · Controlled access and consent management	Scalability of the blockchain network · Privacy and security of sensitive medical data ·Integration with existing healthcare systems
BlockHealth, *ICT International Journal of E-Health and Medical Communications Express (2021)* [14]	Create a blockchain-based system for managing healthcare data	Enhanced data security ·Transparent and immutable healthcare 453ransaction ·Streamlined healthcare processes with smart contracts	Complexity of integrating with existing healthcare systems · Infrastructure requirements for scalability and performance
SEFRA, *International Journal of E-Health Med. Commun.(2020)* [15]	Develop a secure and privacy-preserving data sharing solution in healthcare	Secure and privacy-preserving healthcare data exchange ·Interoperability among healthcare systems ·Patient control over their data	Complexity of implementing privacy-enhancing techniques · Compatibility with existing healthcare infrastructure · Scalability and regulatory compliance
MedSBA, *Journal of Ambient Intell. Humaniz. Comput.(2020)* [16]	Blockchain-based framework for secure sharing and access to sensitive medical and healthcare data	Enhanced security and privacy of medical and healthcare data · Controlled access and consent management	Scalability of the blockchain network ·compliance with healthcare regulations and data protection policies · Integration with existing healthcare systems
Medrec, *International Conference on Open and Big Data.(2017)* [17]	Provide a safe and distributed environment for han dling electronic health records.	Tamper-proof and auditable EHR storage medical records must be shared in a secure and frictionless manner. ·Patients have access to their data.	Scalability of the blockchain network Ensuring data privacy and compliance with regulations like GDPR

Table I. Literature review of previous work.

IV. Proposed Framework and Implementation

We primarily concentrate on two processes in our EHR use case: retrieving and uploading medical data via blockchain. The basic flow of the program is that any third party, including the patient, doctor, lab technician, and other parties, may access BlockFerm. The option to upload records and link them to patients is available to everyone once inside [10]. Any person requesting access can then request permission from the patient. For storing non-sensitive information, the BlockFerm API communicates with the database. The healthcare data is encrypted by BlockFerm using ECC, a public-key encryption method based on the theory of elliptic curves [18]. The codes encrypt_data function creates an ECC cipher using the P-256 curve, exports the public key, and uses the public key to encrypt the data. The upload_file method in the BlockFerm API connects to the IPFS and submits the information to the IPFS. The uploaded file receives a special hash from IPFS that acts as its network identity. The Hash value will then be stored on the Blockchain [19].

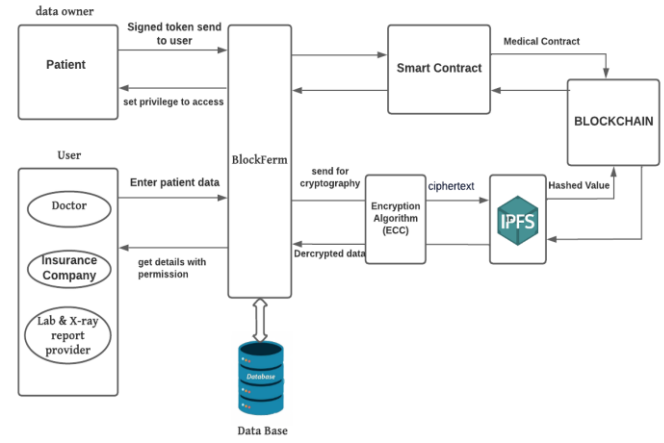

Figure 4. Workflow of Proposed Framework.

- **ECC Encryption:** The study encrypts healthcare data using ECC, a public-key encryption technique based on the theory of elliptic curves. Comparatively speaking to conventional encryption techniques, ECC offers strong security with reduced key sizes. The code's encrypt_data function creates an ECC cipher with the P-256 curve, exports the public key, and uses the public key to encrypt the data[11]. This makes sure that the information is kept private and that only authorized people who have access to the associated private key may decode it.
- **IPFS Integration:** A distributed file system called IPFS makes it possible to store and retrieve files quickly across a decentralized network. The upload_file

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

function in the code establishes a connection with the IPFS daemon and transfers the encrypted data to IPFS. The uploaded file receives a special hash from IPFS that acts as its network identifier[20]. The encrypted data is stored in IPFS, which guarantees data availability and makes it simple to retrieve when needed.

- **Blockchain Integration:** The study uses a blockchain-based approach for managing healthcare data that stores encrypted data together with pertinent information. The Block class holds attributes such as data, temporal shadow value (tsi), nonce, prior hash, patient ID (Pid), and Ethereum blockchain ID (Eid) for each block in the blockchain. It also represents each block in the blockchain. The add_block_to_blockchain function attaches the IPFS hash of the encrypted data to the blockchain, preserving the system's integrity and enabling data tracing[21].
- **Proof of Work:** A proof-of-work process is used to add a block to the blockchain. The method add_block_to_blockchain repeatedly tries various nonce values until a suitable block is discovered that satisfies the proof-of-work requirement[22]. In order to prevent malevolent actors from tampering with the data, the proof-of-work condition, described by int(block.calculate_hash(), target_value, makes sure that each block uploaded to the blockchain involves computational labor.Equations

A. Algorithm 1

Algorithm 1 : Registering a new user in the system

```
struct newuser
    uint256 id
    string name
    uint256 age
Declare an array NewUser[] to store patients structs
Declare a variable userCount to keep track of number of patients
mapping (address => bool) public adminRoles
Define an event named UserAdded, which emits when a new user is added
Parameters:( id, name, age, userAddress)
Define an event AdminRoleAssigned(address indexed admin), which emits wh
an admin role is assigned to an address
modifier onlyAdmin()
    If (adminRoles[msg.sender] == true)
        Only admins can call this function
function addUser(name, age, userAddress)
    Public
    Set uint256 usertId = usertCount++
    Create a new User struct with the usertId, name, age and userAddress
    Append the new user to the users' array
    Emit the UserAdded event with the patient's data

function assignAdminRole(address _userAddress)
    public onlyAdmin
    adminRoles[_userAddress] = true
    emit AdminRoleAssigned(_userAddress)
End
```

This Algorithm defines a User struct to store user data, an array of users, and a counter to keep track of the number of users. The essential function is addUser which allows anyone to add a new user to the blockchain. It takes the user's ID, name, and age as parameters, assigns a unique userId, and emits a UserAdded event[23]. To keep track of which addresses have administrative rights, we use the adminRoles mapping. Only users with admin rights are permitted to call specific functions when the onlyAdmin modifier is used. The contract maker in the constructor is given admin rights by default. Admins can assign admin roles to other addresses using the assignAdminRole function[24].

V. RESULTS AND DISCUSSION

Using an experimental design, we executed several transactions, such as uploading files to examine performance across different file sizes and calculating the cost of completing the transaction through a blockchain network.

Table II. Parity's client performance analysis is inferred by taking processing time and the number of transactions processed by the blockchain system into account

Transaction counts	Blockchain processing time (seconds) without IPFS	Blockchain processing time (seconds) with IPFS
1000	1.84	1.5
2000	3.42	2.41
3000	6.12	4.59
4000	7.21	5
5000	9.47	6.3

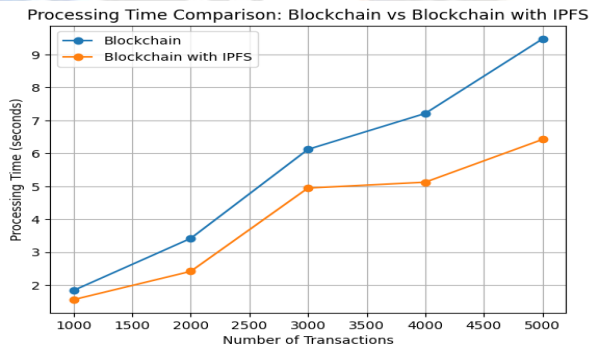

Figure 5. Comparison Analysis of Blockchain with and without IPFS.

The time required to process Blockchain in conjunction with and without IPFS networks is shown in Figure 5[25]. It shows that the number of transactions rose in increments of 1000 to 6,000. When compared to the existing framework, the proposed method has a faster processing time[26].

A. Security Analysis

The effectiveness of the deployed architecture in achieving the previously stated design goals is evaluated below:

*a) **Decentralization:** Owing to blockchain technologies and IPFS, that employ peer-to-peer verification and do deal with centralized oversight, data is decentralized either on and off-chain[27]. Decentralization is the distribution of oversight to end devices rather than a centralized authority. As a result,*

there is no single point of failure and, more importantly, no trust in a centralized authority[28].

*b) **Data security:** A network-based attacker can take advantage of the safety of website login procedures since login credentials are transmitted over HTTP or third-party assets. By using two-factor authorization, this issue can be resolved while also enhancing security[29]. Because two-factor authentication must be completed after entering in to a website, it serves as a safeguard against potential threats by allowing accessibility only after the one-time password (OTP) has been recieved[30].*

Before the information can be transmitted, the device's numerous health factors are evaluated. With the most contemporary updates to security and precautions, this ensures that the device that will transport the information is unaffected in any way[31]. Data is secured with Elliptic Curve Cryptography(ECC) encryption technique and transmitted to the IPFS only once all requirements for the device's health have been met. The solution maintains an unchangeable audit trail of who has accessed which instances of data using blockchain technology[32]. Blockchain technology in electronic health record systems secures data and is virtually impenetrable until a fifty-one percent attack takes place. Furthermore, by providing secure access to records and encrypted transactions, IPFS secures data transfers between peers. Data integrity is guaranteed by the sender's digital signature, and all health information is kept in IPFS using an asymmetric encryption technique[33].

*c) **Role-based access control**: In the suggested method, users are given specific roles through smart contracts, each with their own set of obligations and privileges. It guarantees that users cannot hide their identities by acting as "autonomous entities" that carry out all predetermined actions[34]. For instance, only the admin has the ability to add individuals to the system as well as assign them specific tasks. Users can only access information they either own or are authorized to see as a consequence, and they can only do tasks related to their employment. As a consequence, information confidentiality is ensured[35]For author/s of more than two affiliations:* To change the default, adjust the template as follows.

B. COMPARISON OF THE PROPOSED

TABLE III. COMPARISON BETWEEN EXISTING FRAMEWORKS WITH PROPOSED MODEL.

Feature	[36]	[37]	[38]	[39]	Proposed framework
Integrity	✓	✓	✓	✓	✓
Decentralized Access	✓		✓	✓	✓
Authentication	✓	✓	✓		✓
Availability	✓			✓	✓
Identity Management	✓	✓			✓
Privacy	✓	✓	✓	✓	✓
Flexibility			✓	✓	✓

CONCLUSION AND FUTURE WORK

This study contributes to the creation of a more secure and private blockchain-based health records management system. Sensitive healthcare data may be protected, safely stored, and swiftly retrieved by combining ECC encryption with IPFS. The developed code exemplifies the integration of these technologies, laying the groundwork for future research and advancement regarding medical privacy and the security of information within blockchain ecosystems.

We discussed how blockchain and IPFS technologies may benefit the healthcare business and how they can assist EHR in this paper. Despite developments in the healthcare business and technological advancements in EHR systems, they have encountered several issues with this most recent technology, In addition, the suggested solution focused on lowering document size for uploading through the blockchain network. Furthermore, the unique IPFS hash and user control over EHR provide data immutability.

The study offers a safe and decentralized method for ensuring data integrity in blockchain-based systems. The combination of ECC encryption with IPFS storage improves data security, privacy, and scalability. The suggested method offers up new paths for study into safeguarding confidential information in decentralized apps and Internet of Things (IoT) contexts. However, concerns for ECC key management and IPFS network performance will need to be researched more in the future. There is a great opportunity to study with distributed processing based on blockchain technology, especially with proof-of-work and proof-of-stake protocols in building IoT-based applications.

ACKNOWLEDGMENT

This work is a acknowledged under Integral University manuscript No. IU/R&D/2023-MCN0002250.

REFERENCES

[1] O. Ajayi, M. Abouali, and T. Saadawi, “Secure architecture for inter-healthcare electronic health records exchange,” Sep. 2020, doi: 10.1109/IEMTRONICS51293.2020.9216336.

[2] L. Abdelgalil and M. Mejri, “HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain,” Futur. Internet, vol. 15, no. 3, Mar. 2023, doi: 10.3390/fi15030087.

[3] H. S. Huang, T. S. Chang, and J. Y. Wu, “A secure file sharing system based on IPFS and blockchain,” in ACM International Conference Proceeding Series, Jul. 2020, pp. 96–100, doi: 10.1145/3409934.3409948.

[4] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems,” IEEE Access, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[5] M. Faisal, H. Sadia, T. Ahmed, and N. Javed, Blockchain Technology for Healthcare, no. November 2021. 2022.

[6] M. Kadadha, S. Singh, R. Mizouni, and H. Otrok, “Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. A Context-aware Blockchain-based Crowdsourcing Framework: Open Challenges and Opportunities,” doi: 10.1109/ACCESS.2017.DOI.

[7] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC, Feb. 2018, vol. 2017-Octob, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[8] S. Alam and I. Alshourbaji, "Blockchain-Based Framework for Interoperable Electronic Health Record." [Online]. Available: https://www.researchgate.net/publication/350591357.

[9] S. Al-amin, S. R. Sharkar, M. S. Kaiser, and M. Biswas, "Towards a Blockchain Based Supply Chain Management for E-Agro Business System Towards a Blockchain Based Supply Chain Management for E-Agro Business System," no. December, 2020, doi: 10.1007/978-981-33-4673-4.

[10] R. Kumar, "Scalable Inter-operable and Secure Healthcare Framework For Sharing Patient Medical Report using Blockchain and IPFS Technology," 2022, doi: 10.21203/rs.3.rs-2115239/v1.

[11] A. H. Kashmar, "Encryption key Generation Protocol Based on Elliptic Curve and PSO." [Online]. Available: https://www.researchgate.net/publication/366095384.

[12] R. Bayer, J. Santelli, and R. Klitzman, "New challenges for electronic health records confidentiality and access to sensitive health information about parents and adolescents," JAMA - J. Am. Med. Assoc., vol. 313, no. 1, pp. 29–30, 2015, doi: 10.1001/jama.2014.15391.

[13] E. Daraghmi, Y. Daraghmi, and S. Yuan, "MedChain : A Design of Blockchain-Based System for Medical Records Access and Permissions Management," IEEE Access, vol. 7, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[14] E. Balistri, F. Casellato, C. Giannelli, and C. Stefanelli, "BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten," ICT Express, vol. 7, no. 3, pp. 308–315, Sep. 2021, doi: 10.1016/j.icte.2021.08.006.

[15] R. Charanya, R. A. K. Saravanaguru, and M. Aramudhan, "Sefra: A secure framework to manage ehealth records using blockchain technology," Int. J. E-Health Med. Commun., vol. 11, no. 1, pp. 1–16, Jan. 2020, doi: 10.4018/IJEHMC.2020010101.

[16] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 11, pp. 4613–4641, Nov. 2020, doi: 10.1007/s12652-020-01710-y.

[17] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016, Sep. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[18] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," BMC Med. Inform. Decis. Mak., vol. 20, no. 1, Oct. 2020, doi: 10.1186/s12911-020-01275-y.

[19] A. I. Al Mamun, M. I. Umor Faruk Jahangir, S. I. Azam, M. I. Shamim Kaiser, and A. I. Karim, "A Combined Framework of InterPlanetary File System and Blockchain to Securely Manage Electronic Medical Records."

[20] M. D. Praveen, S. G. Totad, M. Rashinkar, R. Ostwal, S. Patil, and P. M. Hadapad, "Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation," Procedia Comput. Sci., vol. 215, pp. 370–379, 2022, doi: 10.1016/j.procs.2022.12.039.

[21] L. Hang, E. Choi, and D. H. Kim, "A novel EMR integrity management based on a medical blockchain platform in hospital," Electron., vol. 8, no. 4, Apr. 2019, doi: 10.3390/electronics8040467.

[22] T. Alam, "mHealth Communication Framework using Blockchain and IoT Technologies mHealth Communication Framework using Blockchain and IoT Technologies How to cite? Tanweer Alam. "mHealth Communication Framework using Blockchain and IoT Technologies," Int. J. Sci. Technol. Res., vol. 9, no. 6, p. 2020, 2020, doi: 10.31219/osf.io/byvpu.

[23] L. Xu, M. Lin, Y. Feng, and Y. Sun, "BPDST: Blockchain-Based Privacy-Preserving Data Sharing on Thin Client for Electronic Medical Records," J. Comput. Inf. Technol., vol. 29, no. 4, pp. 235–250, 2022, doi: 10.20532/CIT.2021.1005412.

[24] N. Poonguzhali, S. Gayathri, A. Deebika, and R. Suriapriya, "A Framework for Electronic Health Record Using Blockchain Technology," Jul. 2020, doi: 10.1109/ICSCAN49426.2020.9262369.

[25] D. Ray Chawdhuri, "Patient Privacy and Ownership of Electronic Health Records on a Blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11521 LNCS, pp. 95–111, doi: 10.1007/978-3-030-23404-1_7.

[26] S. Athanere and R. Thakur, "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 4, pp. 1523–1534, Apr. 2022, doi: 10.1016/j.jksuci.2022.01.019.

[27] R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, and K. K. R. Choo, "Integrating Privacy Enhancing Techniques into Blockchains Using Sidechains," May 2019, doi: 10.1109/CCECE.2019.8861821.

[28] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and Efficient Data Accessibility in Blockchain Based Healthcare Systems," 2018, doi: 10.1109/GLOCOM.2018.8647221.

[29] M. Alizadeh, K. Andersson, and O. Schelén, "Efficient Decentralized Data Storage Based on Public Blockchain and IPFS."

[30] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Hyperledger healthchain: Patient-centric ipfs-based storage of health records," Electron., vol. 10, no. 23, Dec. 2021, doi: 10.3390/electronics10233003.

[31] N. Poonguzhali, S. Gayathri, A. Deebika, and R. Suriapriya, "A Framework for Electronic Health Record Using Blockchain Technology," 2020 Int. Conf. Syst. Comput. Autom. Networking, ICSCAN 2020, 2020, doi: 10.1109/ICSCAN49426.2020.9262369.

[32] P. Kumar Rangi and P. S. Aithal, "A Study on Blockchain Technology as a Dominant Feature to Mitigate Reputational Risk for Indian Academic Institutions and Universities," no. January, 2020, doi: 10.5281/zenodo.4444329.

[33] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," Wirel. Pers. Commun., vol. 117, pp. 7–25, 2021, doi: 10.1007/s11277-020-07041-7.

[34] M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani, and M. Meraj, "A blockchain framework for secure electronic health records in healthcare industry," Proc. Int. Conf. Smart Technol. Comput. Electr. Electron. ICSTCEE 2020, pp. 605–609, 2020, doi: 10.1109/ICSTCEE49637.2020.9277193.

[35] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE Access, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[36] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain," IEEE Access, vol. 5, pp. 14757–14767, Jul. 2017, doi: 10.1109/ACCESS.2017.2730843.

[37] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," IEEE Access, vol. 6, pp. 53698–53708, 2018, doi: 10.1109/ACCESS.2018.2871170.

[38] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019, pp. 594–601, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00085.

[39] A. H. Mayer, C. A. da Costa, and R. da R. Righi, "Electronic health records in a Blockchain: A systematic review," Health Informatics J., vol. 26, no. 2, pp. 1273–1288, 2020, doi: 10.1177/1460458219866350