IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202040 |

Blockchain Based Electronic Health Record Management System

Prof. Vikas Nandgaonkar, Gaurav Barbhai, Abhijeet Shinde, Aditya Rannaware, Akash Gaygol

Associate Professor, Dept. of C.S., S.C.E.S's Indira College of Engineering and Management, Pune, India

Eng. Student, Dept. of C.S., S.C.E.S's Indira College of Engineering and Management, Pune, India

ABSTRACT: Electronic Health Records (EHRs) are electronically-stored health information in a digital format. EHRs are typically shared among healthcare stakeholders and face power failure, data misuse, lack of privacy, security, and audit trail. On the other hand, blockchain is the revolutionary invention of the twentieth century that offers a distributed and decentralized setting to communicate among nodes in a list of networks without a central authority. It can address the limitations of EHRs management and provide a safer, secured, and decentralized environment for exchanging EHRs data.

Three categories of blockchain-based potential solutions have been proposed by researchers to handle EHRs: conceptual, prototype, and implemented. This study focused on a Systematic Literature Review (SLR) to find and analyze articles submitted either conceptual or implemented to manage EHRs using blockchain. The deep technical analysis focused on evaluating articles based on privacy, security, scalability, accessibility, cost, consensus algorithms, and the type of blockchain used. The SLR found that blockchain technology promises to provide decentralization, security, and privacy that traditional EHRs often lack.

Moreover, results obtained from the detailed studies would provide potential researchers with the type of blockchain for future research. Finally, future research directions, in the end, would direct enthusiasm to combine new blockchain-based systems to manage EHRs properly.

KEYWORDS: Blockchain, Interoperability, Electronic Health Record, Patient-Centric, Transparency, Decentralization

I. INTRODUCTION

In the ever-evolving landscape of healthcare, the integration of blockchain technology into Electronic Health Record Management (EHRM) represents a transformative leap toward security, transparency, and data integrity. Blockchain, originally devised for cryptocurrency, has found a profound application in healthcare by offering an immutable, decentralized ledger for managing electronic health records. This introduction explores the revolutionary potential of blockchain-based EHRM and its implications for the healthcare industry.

1. Ensuring Unprecedented Data Security: Patient records stored on a blockchain are highly resistant to tampering, hacking, or unauthorized access. Any alteration of the data in one block would require simultaneous changes to all subsequent blocks, making fraud virtually impossible.

2. Patient-Centric Control and Ownership: Blockchain empowers patients to take control of their health records. Patients have the cryptographic keys to access and manage their data, deciding who can view or update their records.

3. Seamless Interoperability: The healthcare ecosystem often involves multiple stakeholders, from healthcare providers to insurers. Blockchain offers a standardized and interoperable framework for sharing data across different entities.

4. Trust and Transparency: Transparency is at the core of blockchain technology. All transactions and changes to health records are recorded on a shared ledger visible to authorized parties.

5. Research Advancements: Blockchain facilitates the sharing of anonymized patient data for medical research, without compromising privacy. Researchers can access aggregated, real-world patient data to advance medical science.

6. Compliance and Privacy: Blockchain-based EHRM systems can align with privacy regulations such as HIPAA in the United States, GDPR in Europe, and similar laws globally.

International Journal of Innovative Research in Computer and Communication Engineering

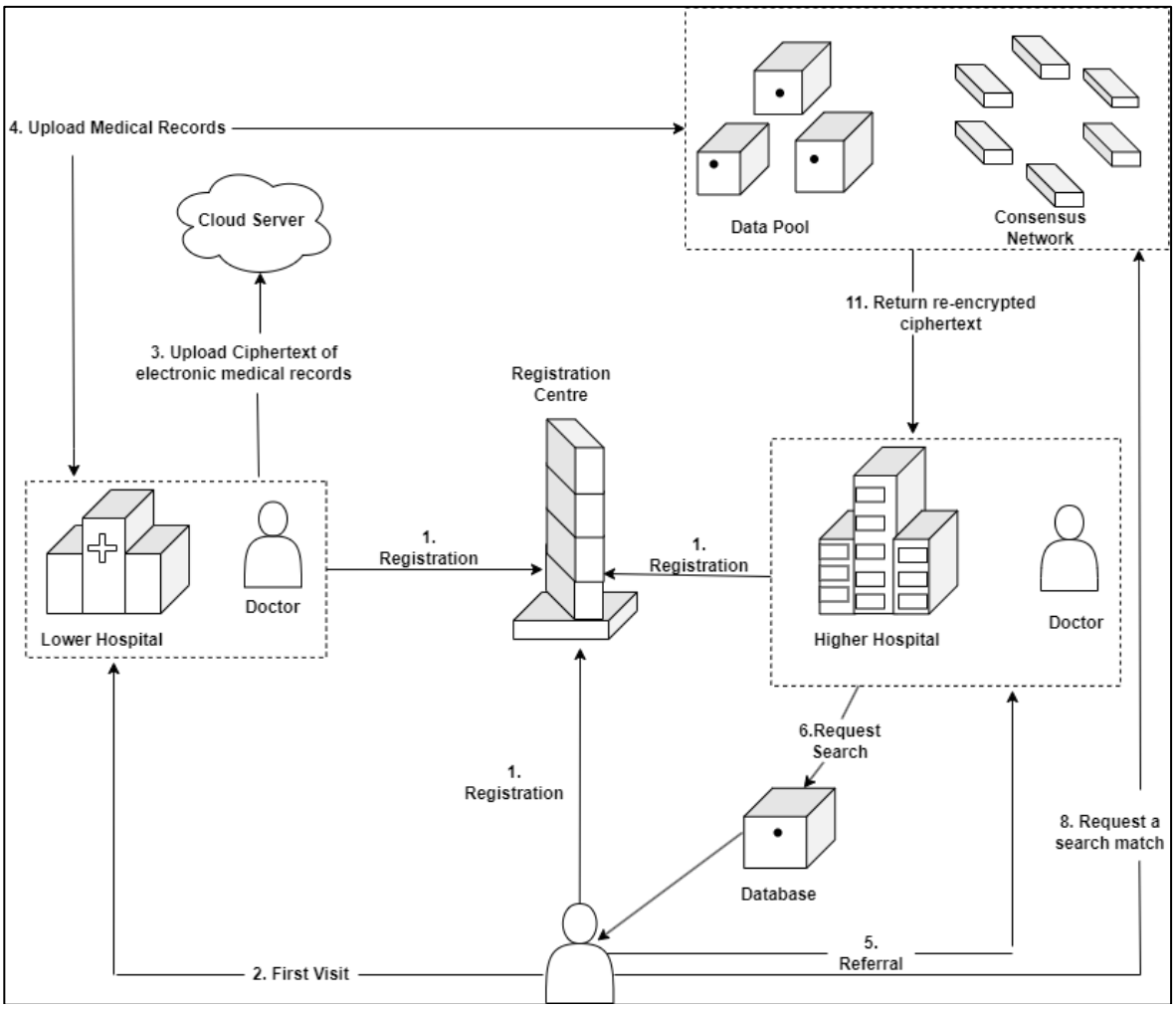
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202040 |

II. RELATED WORK

The scheme contains six entities, which are registration center, query manager, patient, medical institution, consortium blockchain, and cloud server. These entities interact with each other to provide data control and protection service in the exchange of medical record information. There are four phases in the scheme proposed, user registration, data storage, request access, and request processing. In this figure, interaction 1 and interaction 2 are the user registration phase. Interactions 3 and 4 are the data storage phase, interactions 5, 6, 7, and 8 are the request access phase, and interactions 9, 10, and 11 are the request processing interaction.



(1) Registration Center: The entity is used to generate and store keys. The registration center is responsible for generating the public parameters of the system, that is, the master key when the system is initialized.Users' identity materials will be safely stored in the registration center, and the SHA256 hash of the public key will be transmitted to the consortium blockchain for backup.
(2) Query Manager: The entity receives a request and authenticates the user to determine that he is a legitimate user of the system. Meanwhile, the entity formats the request in a standard manner and then forwards it to other users or the consortium blockchain network.
(3) Patient: Patients should register in the system when they first visit the hospital for stroke, and the registration centre allocates a public-private key pair for encrypting electronic medical records and a symmetric key for generating pseudonyms for each patient. Patients can grant doctors access to relevant data, set the time limit for record access, and revoke his authorization at any time.
(4) Medical Institution. The entity is responsible for uploading electronic medical records and is subject to the supervision and management of the regulatory Cloud server Patient Registration CenterWhen medical institutions are

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202040 |

registered in the blockchain, strict audit standards are required. And then doctors encrypt, sign, and finally send the records to the cloud server. Medical record indexes and abstracts are sent to the consortium blockchain for storage on the chain. When a doctor at a higher-level hospital requests a medical record search, he needs to be authenticated to get patient authorization.

(5) Cloud Server: Due to the practical limitations of cost, storage capacity, and other factors, large-scale medical data is encrypted and stored outside the blockchain. The cloud server is used to store the ciphertext of electronic medical records uploaded by the doctor from the client, thereby reducing the storage pressure of the blockchain After receiving the ciphertext request from the blockchain, the ciphertext of the electronic medical record is returned to the blockchain master node for proxy re-encryption.

(6) Consortium Blockchain. The consortium blockchain network is composed of nodes of various medical institutions. The stroke medical treatment combination includes multiple levels of medical institutions, including tertiary hospitals, second-level hospitals, and community hospitals. Each hospital acts as a node with different functions in the consortium blockchain network according to the level. In the process of sharing medical records, after receiving the search trapdoor sent by the patient, the main node of the consortium blockchain performs search matching and sends a ciphertext request to the cloud server according to the matched index address. After receiving the ciphertext data returned by the cloud server and the reencryption key transmitted by the patient, the consortium chain master node acts as an agent to reencrypt the ciphertext data and convert it into a ciphertext that the doctor user can decrypt with the private key.

III. MATHEMATICAL MODEL

The patient submits a new medical record by calling the submitRecord function of the Patient Record smart contract (by issuing a transaction on the Ethereum blockchain), as described in detail in Algorithm 1.

Algorithm 1submitRecord: Submit New Medical Record

1. **Input**: new bundle hash b#
2. **Require**: owner patient only
3. Push b# to array of uploaded bundle hashes **B#**
4. Create new record r with empty requests list
5. Add r to array of records R
6 **Emit:** inform patient about successful record addition

Once a doctor wants to access a certain record of the patient, the doctor needs to call a request Record function of the Patient Record smart contract, as discussed in Algorithm 2.

Algorithm 2 requestRecord: Request Medical Record

1. **Input**: medical record r, doctor public key $\mathbf{k^p_D}$, oracle range $\mathbf{O_{min}}$, $\mathbf{O_{max}}$
2. **Require**: function caller is a doctor
3. **Require:** valid $\mathbf{k^p_D}$
4. **Require**: $0 < \mathbf{O_{min}} \leq \mathbf{O_{max}}$
5. Create new request q with the attributes of the doctor address, current time, specified $\mathbf{O_{min}}$ and $\mathbf{O_{max}}$ parameters, false grant status, and false oracles evaluated status
6. Add q to the array of requests Q located inside of r
7. r.c ← r.c + 1, where r.c is the number of requests for the medical record r
8. **Emit:** inform patient about $\mathbf{k^p_D}$
9. **Emit:** inform doctor about function execution result

The function takes several parameters to identify the desired medical record, the public key of the doctor, and the acceptable range of the number of oracles. The function verifies that the doctor supplied the correct public key by computing its hash, and performing a bit-wise AND operation with $\mathbf{2^{20\times8-1}}$, then ensuring the result is equal to the doctor Ethereum address. The exponent in $\mathbf{2^{20\times8-1}}$ refers to the number of bits in an Ethereum address, which is 20 bytes. The function also ensures that the caller is a doctor, and the range of the number of oracles is valid. A new request structure is then created with the appropriate attributes provided by the doctor, which gets added to the array of requests in the patient's medical record. The function ends with informing the patient about the doctor's public key, such that the patient can generate the re-encryption oracle, and informs the doctor about the status of the execution result.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

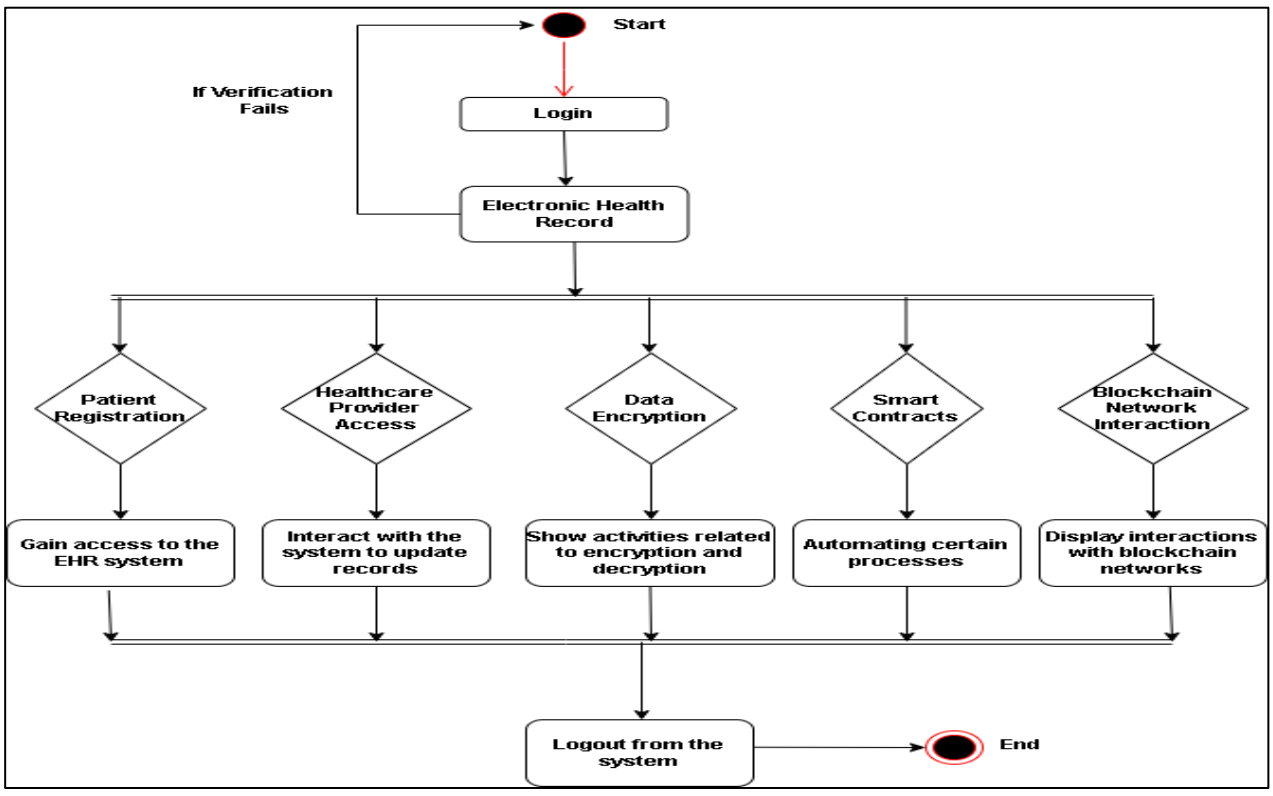
| DOI: 10.15680/IJIRCCE.2024.1202040 |

The oracles subsequently call the addOracleResponse function described in Algorithm 3. At this step, oracles request the medical record bundles from the IPFS by sending the bundle hash, then compute the hash of the encrypted symmetric key (found in the bundle) and send the result to the PRSC. Depending on the latency and correctness of the oracle response, the oracle is evaluated by the smart contract. This is performed by linearly mapping the oracle's latency to the range between 1 and 65,535. 1 is the minimum positive value in unit 16, and in our case, it is used to indicate the highest latency (which we chose to be 1 hour). 65,535 is the maximum value in uint16, and in our case, it is used for minimum latency, which is 1 second. The initial value for the reputation is 32,768, which in this range's midpoint.

Algorithm 3 addOracleResponse: Submit an Oracle Response

1. **Input:** request q, response hash $\mathbf{k^{O}_{sP}\#}$
2. **Require:** q is granted by patient
3. **Require:**qs = false, where qs is the evaluation status of the request
4. l ← t0 − tq where l is the latency, t0 is the current time, tq is the request time
5. Considering qO is array of participating oracles. . .
6. **If** len(qO) <Omin or (len(qO) ≥ Omin **and** len(qO) <Omax and l ≤ 1 hour) **then**
7. c ← ($\mathbf{k^{O}_{sP}\#}$= $\mathbf{k_{sP}\#}$), where c is boolean to evaluate correct response, and ksP# is the correct hash
8. n ←(2^{16}(l-1)/1 hour – 1 second) + 2^{16}-1, where n is the oracle rating
9. n ← n × c
10. Add oracle o to q_O
11. Add n to array of ratings of the participating oracles N
12. **end**
13. if len(q_O) ≥ Omin and l > 1 hour **or** len(q_O) = Omax **then**
14. qs ← true
15. Call evaluateOracles
16. **end**

IV. ACTIVITY DIAGRAM



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202040 |

Activity Diagram:
The activity diagram depicts the workflow involved in managing patient electronic health records (EHRs) within a Blockchain-based EHR system. It illustrates the interactions between various system components and users, highlighting the secure and transparent nature of blockchain technology in healthcare data management.

- **Main Activities:**
  1. **Patient Registration:** The system begins with patient registration, where new patients are added to the system. This involves verifying patient identity, collecting personal information, and assigning unique patient IDs.
  2. **EHR Access Request:** A healthcare provider initiates the process of accessing a patient's EHR by submitting an access request. This request specifies the patient's ID and the desired access level, such as read-only or read-write.
  3. **Access Authorization:** The system verifies the healthcare provider's credentials and evaluates the access request. If the request is valid, the system grants access based on the requested level.
  4. **EHR Access and Interaction:** Upon receiving access, the healthcare provider can view, modify, and update the patient's EHR. This includes adding new health data entries, modifying existing data, and reviewing past records.
  5. **Data Storage on Blockchain:** All EHR data modifications are securely stored on the blockchain, creating an immutable and tamper-proof record of patient health information.
  6. **Access Revocation:** If access to an EHR is no longer needed or the healthcare provider's credentials change, the system can revoke access, preventing unauthorized access to patient data.
  7. **Audit Trail and Traceability:** The blockchain provides an audit trail of all EHR data modifications, enabling traceability and ensuring accountability for data changes.
- **System Components:**
  1. **Patient Database:** Stores patient information, including names, IDs, and contact details.
  2. **EHR Database:** Stores patient health data, including diagnoses, medications, and treatment plans.
  3. **Blockchain Network:** A distributed ledger that securely stores EHR data modifications.
  4. **Access Control Mechanism:** Enforces access restrictions based on user roles and permissions.
  5. **Audit Trail Management:** Tracks and records all EHR data modifications for future reference.

V. CONCLUSION AND FUTURE WORK

We will provide a solution for supply chain management for medicines. Our Project also addresses the critical issues such as data storage scalability. We are committed to developing innovative data management solutions for patients, including those in comas, illiterate individuals, and even deceased patients, ensuring that their healthcare data is handled with utmost care and sensitivity. Our project endeavours to establish a standard format for healthcare data sharing and storage that is both practical and secure.
We are planning the integration of Internet of Things (IoT) devices and wearables into EHR systems can provide real-time health data, enabling proactive healthcare interventions. Future work should aim to seamlessly incorporate data from these devices into blockchain-based EHRs, ensuring data accuracy and security.

REFERENCES

[1] E. Chukwu and L. Garg, ‘‘A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations,’’ IEEE Access,vol. 8, pp. 21196–21214, 2020.
[2] A. Fernandes, V. Rocha, A. F. D. Conceicao, and F. Horita, ‘‘Scalable architecture for sharing EHR using the hyperledger blockchain,’’ in Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C), Mar. 2020, pp. 130–138.
[3] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, ‘‘Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity,’’ in Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 310–317.
[4] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, ‘‘A patient-centric health information exchange framework using blockchain technology,’’ IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, Aug. 2020
[5] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, ‘‘A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud,’’ IEEE Access, vol. 8, pp. 170713–170731, 2020.
[6] O. Ajayi, M. Abouali, and T. Saadawi, ‘‘Secure architecture for interhealthcare electronic health records exchange,’’ in Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS), Sep. 2020, pp. 1–6.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202040 |

[7] V. Jaiman and V. Urovi, ‘‘A consent model for blockchain-based health
data sharing platforms,’’ IEEE Access, vol. 8, pp. 143734–143745, 2020.
[8] A. Shahnaz, U. Qamar, and A. Khalid, ‘‘Using blockchain for electronichealth records,’’ IEEE Access, vol. 7, pp. 147782–147795, 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details