

Optimized Blockchain Based Decentralized Framework for Electronic Health Records [†]

Sandip Bankar ^{1,*}, Surekha Janrao ², Rohini Patil ³, Shweta Kukreja ⁴ and Aruna Pavate ⁵

¹ SVKM's NMIMS Navi Mumbai, Mumbai 400056, India

² DJSCOE Mumbai, Mumbai 400056, India; surekha.janrao@djsoe.edu

³ TEC Navi Mumbai, Navi Mumbai 400706, India; rohinipatil@ternaengg.ac.in

⁴ Amity University Mumbai, Mumbai 410206, India; swetakukreja@gmail.com

⁵ SFIT Mumbai, Mumbai 400103, India; arunapavate@sfit.ac.in

* Correspondence: bankar.sandip@nmims.edu

[†] Presented at the 2nd International Electronic Conference on Processes: Process Engineering – Current State and Future Trends (ECP 2023), 17–31 May 2023; Available online: <https://ecp2023.sciforum.net/>.

Abstract: Electronic Health Record's (EHR) information verification, synchronization, sharing, and storage are challenging for the medical system. Distributing data safely while protecting customer privacy becomes an issue. Blockchain has been suggested as a secure data exchange solution due to its immutability feature. This paper proposes a blockchain-enhanced, decentralised electronic medical records system. The proposed system validates and stores electronic medical data on the blockchain by hashing it. The InterPlanetary File System encrypts and stores encrypted electronic medical data to solve the blockchain's scalability issue. Medical health systems generate many records; the proposed system stores all records as blockchain transactions. A blockchain ledger could make data accessible to authorised users, improving visibility and growth awareness during therapy. To optimise the performance of the proposed system, performance bottlenecks are identified and solutions are proposed. We have used optimal endorsement policies and blockchain code-level changes. When performance is compared to other blockchain networks, the proposed network outperforms them. Transaction throughput and latency outperform by 13% and 8%, respectively, while addressing stakeholder security and trust concerns.

Keywords: blockchain; InterPlanetary file system; health records

Citation: Bankar, S.; Janrao, S.; Patil, R.; Kukreja, S.; Pavate, A. Optimized Blockchain Based Decentralized Framework for Electronic Health Records. *Eng. Proc.* **2023**, *37*, x. <https://doi.org/10.3390/xxxxx> Published: 17 May 2023



Copyright: © 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Electronic medical records, medical images, diagnostic reports, infectious diseases, and other types of data are generated daily as a result of the rapid development of information technology. With the right use of these data, infectious diseases can be predicted in advance so that precautions can be taken, but they can also be used as legal evidence in disputes over medical or personal matters. Therefore, it is worthwhile to research how to effectively utilise medical data. Electronic medical records can represent a patient's current state of care quickly and accurately, as well as share treatment experiences with other healthcare facilities. However, the patient's privacy would be compromised once the provided medical data were utilised unlawfully [1]. Controlling the right to access medical data is therefore a pressing concern. Technology's recent advancements are changing how we use and perceive things, which has an impact on every aspect of human life. Similar to the improvements technology has brought about in a number of other spheres of life, it is also discovering new methods to advance the healthcare industry. The key advantages that technological advancements are bringing to the healthcare industry include improvements in security, user experience, and other areas. Medical, or EHR (Electronic Health Record), and EMR (Electronic Medical Record) systems provided these

advantages. Nevertheless, they continue to have certain problems with data integrity, user ownership of data, and the security of medical information. The application of a cutting-edge technology, such as blockchain, may be the answer to these problems [2]. With the use of this technology, medical records and other information connected to healthcare might be stored on a safe, impermeable platform.

2. Limitations of Existing Work

Blockchain technology has also been mentioned as a potential solution by several researchers [3,4]. Many of the solutions rely on retrieving data from cloud servers, yet most cloud servers are cynical and half-honest. Additionally, the current blockchain medical data recovery solution lacks comprehensive answers for both data owners and consumers. The aforementioned article's major goals are to set up access control mechanisms for medical records and provide control over personal health information. However, the performance of blockchain-based health record systems has not been the main focus of the majority of solutions. In this research, we provide an effective privacy-preserving decentralised access control system that makes use of blockchain technologies to improve access control policy administration in order to solve these shortcomings. By suggesting the hybrid level of the decentralised access control model, which takes into account both the "role" concept and the "attributes," our approach differentiates from prior research. Because of this, maintaining security and privacy with effective access control measures is still a crucial problem, which is what we try to do in our work. The most effective method for implementing access control at the moment is attribute-based encryption (ABE) [5–8]. Medical facilities outsource the maintenance of encrypted patient data to a third party (a cloud server), which lowers the cost of computing, frees up local storage, and allows for quick data retrieval. The use of blockchain technology in contemporary healthcare facilities has also gained popularity [9,10]. However, medical data saved on the blockchain cannot be easily accessed. The cloud server is centralised, so if one cloud model fails, the entire cloud server will become unavailable. Literature [11] and [12] combine the blockchain with the cloud server to address how to recover data while also addressing how to provide a safeguard for data security. We consider the InterPlanetary File System (IPFS) as our storage platform to address this issue.

3. Contribution

This study proposes a patient-privacy-preserving EHR sharing strategy using hospital servers and permissioned blockchains.

- **Audit System:** The audit method authenticates doctors, prevents them from uploading patients' electronic health records to the hospital server under a false name, and ensures the data's validity and dependability.
- **Content Security:** Our model stores medical data on an IPFS, which allocates a unique hash for each file, so files cannot be stored repeatedly while saving storage space.
- **Keyword Search:** In our method, users may rapidly discover medical documents using keywords and check their legitimacy and source. EHR immutability and sharing are also achieved.
- **Controlled Access:** We assign user-specific access privileges to prevent unrelated people from seeing the patient's medical history. The user can decode the ciphertext only if their private key matches the access policy. This study proposes a patient-controllable EHR sharing approach to protect its privacy as patients don't completely understand how to utilise their EHRs. EHR integrity is vital since it includes sensitive data. This protects integrity and auditability during data transfer.

Rest of the paper is organized as follows. Section 4, explains proposed methodology. In Section 5, the performance analysis model is discussed and a performance comparison is shown, followed by a conclusion and future scope.

4. The Proposed System

The goal of this method is to develop a system in which blockchain could also reinvent the way patients’ electronic health records are stored and shared by providing safer and more secure mechanisms for patient health information exchange of medical data in the healthcare and medical industry. In this section, we elaborate on the design goal of the proposed EHR data-sharing model and focus on explaining the logical framework and running process of the model.

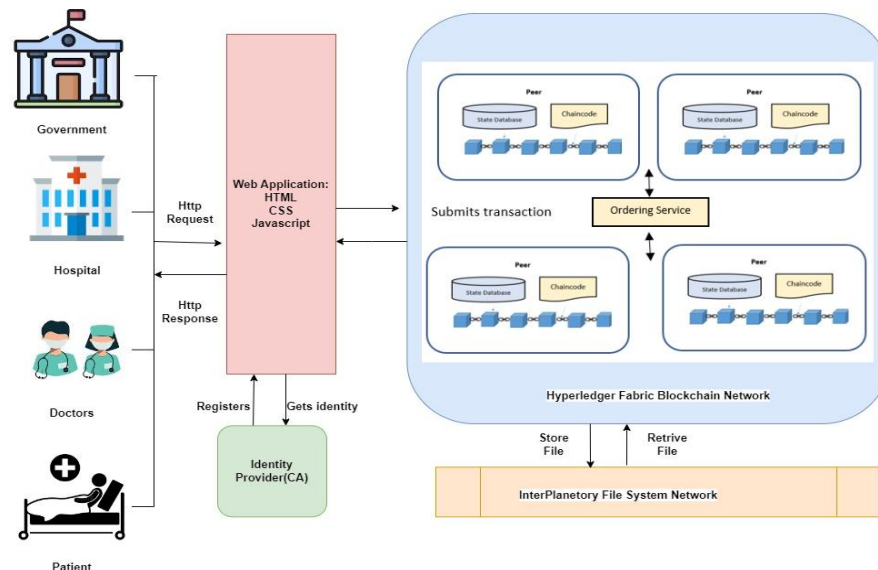


Figure 1. Framework for the proposed system.

The prototype was built by taking into consideration the number of active hospitals and creating a scaled network of five organisations. Each of these five organizations is represented by an Hyperledger Fabric(HL) organization holding two peer nodes, one orderer node, and a custom Certificate Authority (CA) to issue certificates to its members. The different components are processes running in each hospital’s infrastructure. The hospitals can use the prototype both as a backup mechanism to be integrated with their legacy systems and as a full operating system meant to substitute the current solutions. The prototype allows different entities to access and operate the system and the records. Each entity has different importance and freedom within the system. This freedom reflects in the operations that an entity can perform: some have access and rights over the patient records, and some have the faculty to modify system policies and rules. The HL Fabric network must ultimately approve the vast majority of these operations and rights through the consensus process.

The prototype supports the following roles:

- Government: monitors the system and can change the mode;
- Hospital: can create, retrieve, update, delete a record, and ask for consent;
- Doctor: can read and update records, ask for consent;
- Patient: read their health record, and give consent to the doctor.

The EHRs are expressed as JSON files, and the entities interact with them through a smart contract that represents and guards the data model. The contract not only represents the EHR but also defines the operations that can be performed over it. The functions to interact with the EHR listed as follows:

- Create a health record: *createRecord({key: value}): patientId* This function accepts a key-value asset that could be either a JSON file or Javascript object. It returns a string containing the patient identification.
- Retrieve a record: *getRecord (patientId): medicalRecord* Given a patient identification number, this function returns a JSON file containing the EHR corresponding to the id.
- Update a record: *updateRecord (patientId, {key: value}): Boolean* This function allows a patient to modify the content of her record: it accepts the patient id and the field that must be modified, and returns the boolean result of the operation.
- Delete a record: *deleteRecord (patientId): boolean* This function allows to removal a record given the patient id.
- Request for treatment: *requestForTreatment (patientId, doctor): Promise* A practitioner (doctor, physician, etc.) or an organization can request to access or create a record belonging to a patient. The patient gets notified and can either accept or decline the request.
- Treat patient: *treatPatient (patientId, diagnosis, doctor, treatment): ! boolean* The doctor that has the right to access a record, can update its information through this function.
- Give consent: *giveConsent (patient, doctor): boolean* With this function, the patient can grant someone the right to access and modify her record. The entity can be either an organization or someone representing the organization such as a doctor or a nurse.

5. Performance Analysis and Discussion

In this part, blockchain benchmarks and evaluation metrics are used to evaluate and analyse the performance of the proposed architectural framework. The outcomes are examined using criteria including block size, endorsement policy, and block generation time, among others.

Throughput, latency, and other characteristics are used to do performance evaluations for various scenarios. The benchmarking tool used for network-based blockchain application examination is called Hyperledger Caliper [13]. The performance evaluation framework consists of a caliper manager along with workers who provide workload to the proposed system. It follows the steps shown in the framework, which result in test reports. Several variables, including latency, throughput, CPU use, incoming and outgoing traffic, memory consumption, disc write and read, network I/O, etc., are tracked in order to assess the framework's performance. Block size, transaction per second (TPS), support mechanism, channel, resource consumption, and record database configuration parameters are modified based on the evaluation.

5.1. Impact of Hyperledger Fabric Block Parameters on Performance

The endorsement policy, the frequency of reads and writes in a single transaction, and the total number of transactions in a block are all crucial aspects that affect blockchain performance. We investigated the performance of Hyperledger Fabric to pinpoint the bottlenecks and motivate improvements in our proposed system. To optimize transactional performance, bottlenecks, and areas are studied, and their impacts are analyzed.

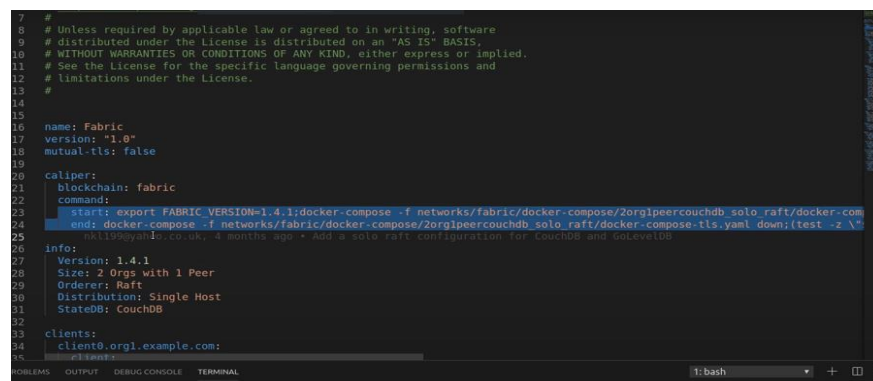
The impact of different load generation rates and block sizes on performance is also explored. The proposed system also demonstrates how block size and endorsement policy affect performance metrics like throughput and latency.

- **Block Size Effect:** Before adding any transactions to a block, they get verified. Then the client requests permission from several endorsing peers before sending the transaction proposal. The transaction is deemed genuine only after it has received approval from the required number of peers. All engaged endorsing peers' certificates, public keys, and signatures are collected together with the transactions for further verification. The block size parameter plays a key role in validating transactions, so configuring this parameter is necessary as the number of transactions increases.

- **Effect of Endorsement Policy:** Endorsement policies are used in Fabric to determine which peers must approve a transaction before any sent transaction is deemed genuine and added to the ledger. Several ramifications of Fabric’s endorsement policy component are examined in this paper. This work uses updated endorsement policy strategies to improve performance. The effect of the endorsement policy on the operation of the Hyperledger fabric is examined, we must define the endorsement policy with fewer sub-policies and endorsers in order to attain greater performance. Moreover, NOutOf policy always performs better than And/Or policy but is less effective.
- **Impact of Types of Transactions on Block Size:** The number of input transactions in a block cannot be expected to remain constant, so different blocks may have different sizes. Transactions can be read or written, depending on the type of transaction. Read transactions must produce the current state. So block size has no effect on read transactions; it can only be executed with write transactions. It’s critical to configure the block size to be smaller when the transaction arrival rate is below the saturation threshold. Also, it is important to increase the block size when the transaction arrival rate exceeds or equals the saturation point.

5.2. Experimental Evaluation

In this research paper, we have conducted a comprehensive performance benchmarking of the proposed system and compared it with Hyperledger Fabric v1.4. Figure 2 shows the configuration file used for Hyperledger caliper with hyperledger fabric 1.4. The architecture of the system is used as a system under test to check the performance of hyperledger Fabric. The results are examined in this part using criteria such as block formation time, endorsement policy, block size, and so on. The benchmark tool Hyperledger caliper will be used to analyse the created blockchain-based apps over the network. This section evaluates the present system’s performance using blockchain assessment metrics. The Hyperledger Caliper benchmarking framework is used to monitor performance, and the results are analyzed using metrics such as Success Rate, Send Rate (TPS), Throughput (TPS), and Latency (S) [15]. The performance of the proposed system is measured using Caliper, which is given 500, 1000, 1500, 2000, and 2500 active rounds of trading split into three subdivisions at variable interest rates. A blockchain system’s throughput is defined as the rate at which it can commit a certain number of valid transactions. The term “Transaction Latency” refers to the time it takes for a transaction to become effective across the network.



```

7 #
8 # Unless required by applicable law or agreed to in writing, software
9 # distributed under the License is distributed on an "AS IS" BASIS,
10 # WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
11 # See the License for the specific language governing permissions and
12 # limitations under the License.
13 #
14 #
15 #
16 name: Fabric
17 version: "1.0"
18 mutual-tls: false
19
20 caliper:
21   blockchain: fabric
22   commands:
23     start: export FABRIC_VERSION=1.4.1;docker-compose -f networks/fabric/docker-compose/2org1peercouchdb_solo_raft/docker-com
24     end: docker-compose -f networks/fabric/docker-compose/2org1peercouchdb_solo_raft/docker-compose.tls.yaml down;(test -z $V
25     nk119@yan10.co.uk: 4 months ago • Add a solo raft configuration for CouchDB and goleveldb
26
27 info:
28   Version: 1.4.1
29   Size: 2 Orgs with 1 Peer
30   Orderer: Raft
31   Distributions: Single Host
32   StateDB: CouchDB
33
34 clients:
35   client0.org1.example.com:

```

Figure 2. Caliper configuration with Hyperledger Fabric 1.4.

Transaction Throughput(TT) = Total Committed Transaction(TCT)/Total time in sec-Non Committed Transaction(TTS)

Transaction Latency(TL) = Confirmation Time(CT)*Network Threshold(NT)-Submit Time for transaction(ST)

For performance comparison, Hyperledger Fabric 1.4 network is considered as per the Hyperledger documentation [14] compared with our proposed system after optimization at validation and channel phase of blockchain. These graphs show that the proposed system outperforms the hyperledger system in terms of throughput and latency when the system is tested with 100, 500, 1500, 2000 and 2500 number of transaction which is shown in Figures 4 and 5. The proposed system is found to be more efficient in terms of transaction throughput and latency by 13% and 8%, respectively.

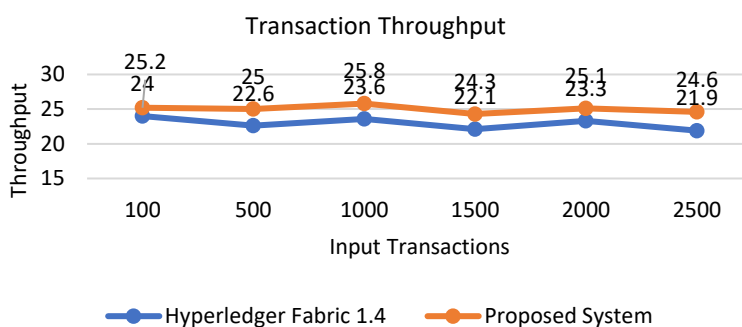


Figure 3. Comparison of Throughput of Hyperledger Fabric and proposed system.

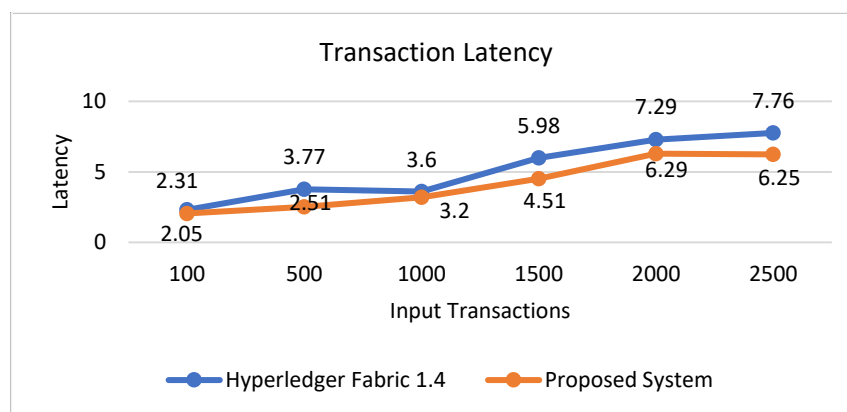


Figure 4. Comparison of latency of Hyperledger Fabric and proposed system.

6. Conclusions

Using Blockchain in healthcare systems has become increasingly essential in recent years. In addition to lowering the possibility of cybercrime, it may also lead to data verification, data rectification, and safe data provision. Redundancy and fault tolerance in the system also facilitate the distribution of data. In this research, we recommend a system architecture for an access control policy for participants to protect the confidentiality of medical records stored on a distributed ledger technology Blockchain. The proposed system integrates strict access controls with safe record-keeping. It makes a user-friendly system that anyone can pick up and utilise. Since the framework makes use of IPFS’s off-chain storage method, it also offers ways to guarantee the system solves the storage challenge. The proposed system is also optimized and found to perform better when performance is evaluated concerning similar systems. Swarm Hash will be used in the future inside the proposed framework. You can retrieve data from multiple nodes at once in the Swarm (Decentralised Data Storage and Distribution), and as long as any one node hosts a given piece of data, it will continue to be available everywhere. Files are addressed using a hash of their contents.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dash, S.; Shakyawar, S.K.; Sharma, M. Big data in healthcare: management, analysis and future prospects. *J. Big Data* **2019**, *6*, 54. <https://doi.org/10.1186/s40537-019-0217-0>
2. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. ISSN 1110-8665,
3. Srivastava, G.; Dwivedi, A.D.; Singh, R. PHANTOM Protocol as the New Crypto-Democracy. In *Computer Information Systems and Industrial Management*; Saeed, K., Homenda, W., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 499–509.
4. Srivastava, G.; Dwivedi, A.D.; Singh, R. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, Porto, Portugal, 26–28 July 2018; pp. 508–513.
5. Buccafurri, F.; Fotia, L.; Lax, G. Social Signature: Signing by Tweeting. In *Electronic Government and the Information Systems Perspective*; Kó, A., Francesconi, E., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 1–14.
6. Buccafurri, F.; Fotia, L.; Lax, G. A privacy-preserving e-participation framework allowing citizen opinion analysis. *Electron. Gov. Int. J.* **2015**, *11*, 185–206.
7. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303.
8. Qu, C.; Tao, M.; Yuan, R. A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes. *Sensors* **2018**, *18*, 2784.
9. Kaushal, R.; Shojania, K.G.; Bates, D.W. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch. Intern. Med.* **2003**, *163*, 1409–1416
10. Schiff, G.D.; Hasan, O.; Kim, S.; Abrams, R.; Cosby, K.; Lambert, B.L.; Elstein, A.S.; Hasler, S.; Kabongo, M.L.; Krosnjar, N.; et al. Diagnostic error in medicine: analysis of 583 physician-reported errors. *Arch. Intern. Med.* **2009**, *169*, 1881–1887
11. Cachin, C. *Architecture of the Hyperledger Blockchain Fabric, Workshop on Distributed Cryptocurrencies and Consensus Ledgers*; IBM Research: Rüschlikon, Switzerland, 2016; Volume 310.
12. Cachin, C. *Architecture of the Hyperledger Blockchain Fabric: Workshop on Distributed Cryptocurrencies and Consensus Ledgers*; IBM Research: Rüschlikon, Switzerland, 2016; Volume 310.
13. Caliper, Hyperledger. Available online <https://www.hyperledger.org/projects/caliper> (accessed on 15 February 2023).
14. Fabric, Hyperledger. Available online <https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatsnew.html> (accessed on 20 February 2023).
15. Bankar, S.; Shah, D. Decentralized Framework to Strengthen DevOps Using Blockchain. In *Computational Intelligence. Lecture Notes in Electrical Engineering*; Shukla, A., Murthy, B.K., Hasteer, N., Van Belle, J.P., Eds.; Springer: Singapore, 2023; Volume 968. https://doi.org/10.1007/978-981-19-7346-8_44.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.