International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

PRIVACY AWARE AND INTEROPERABLE PATIENT DATA STORAGE AND SEARCHING USING BLOCKCHAIN

[1]Faiza Aurang Zeb, [2]Syed Owais Shah, [3]Osama Al Rahbi, [4]Mohammad Babar, [5*]Muneeba Darwaish, [6*]Suliman Khan

1 Department of Computer Science, Govt. Girls Post Graduate College Mandian, Abbottabad.

2,5 Department of Telecommunication, Hazara University, Mansehra, Pakistan.

3,4 Department of computing and Electronics Engineering, Middle East College Muscat, Oman.

6 Department of Software Engineering, Dalian University of Technology, Dalian, 116024, China.

[*]Corresponding Author: Muneeba Darwaish. Email: muneebadarwaish@gmail.com and Suliman khan. Email: sulimankhan@mail.dlut.edu.cn

Abstract

Healthcare data are highly sensitive data it must be managed with strict security and reliability. Increasing concerns regarding personal health continue to create major challenges for the healthcare sector, particularly within Electronic Medical Record (EMR) systems. Because medical events may occur across different locations, patient information often becomes fragmented among multiple healthcare providers. As a result, patients frequently lose access to their historical records, and healthcare institutions struggle with issues related to interoperability, searching in blockchain ledgers, and secure data storage. To address these challenges, this paper proposes "HealthSearchin" breadcrumb searching mechanism and a conceptual single system architecture for Electronic Health Records (EHRs) using blockchain technology. The system integrates encrypted cloud storage with a permissioned blockchain, specifically Hyperledger Fabric, which is partitioned into specialized clusters to enhance scalability and privacy. Performance evaluation demonstrates that the system achieves a throughput of approximately 600 transactions per second with an optimal block size of 1MB, and an average block creation time of 20ms for patient registration. Moreover, the breadcrumb search time grows gradually from approximately 3ms to 24ms as the number of matched documents increases from 50 to 1,200. The cluster-based architecture, coupled with an indexed-based "breadcrumb" search mechanism, significantly improves data retrieval efficiency and system scalability. These testing results confirm that the proposed framework is a practical and effective solution for healthcare contexts, successfully addressing critical issues of storage, interoperability, and efficient data retrieval.

Keywords: Blockchain, Electronic Health Record, HealthSearchin, Searchable Encryption, Permissioned Blockchain, Hyper ledger Fabric.

1. INTRODUCTION

Healthcare data is one’s personal asset and it should be controlled, managed, and owned by the

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
patient (Navaz et al., 2021). A good and reliable healthcare system is the most needed and demanded facility in today's world, which would serve citizens with the latest and most advanced care provider technologies (Swetha et al., 2020). The provision of healthcare is among the most crucial aspects of a person's existence, where patients' data must be wisely stored while maintaining data transparency (Drew Ivan, 2016). Earlier, patients' healthcare data stored on different healthcare providers' private databases cannot be shared among different healthcare providers' private databases. The main issue in these local databases is unreliability, because if the data is lost from local database in any case, then there is no additional backup storage for that data. Secondly, if any healthcare provider has its data stored at its local database, it is hard to find that particular patient's data at another local healthcare provider. As healthcare systems move toward more digitalized architectures, for healthcare data sharing, cloud-based solution is being utilized, which is efficient in term of storage, economy, scalability, flexibility, and computation but questionable in term of trustworthiness, privacy, and ownership, because of third party involvement and dependency (Gavrilov et al., 2018).

Following recent technological developments in health data management, blockchain technology has been widely used in healthcare systems. Implementing blockchain-based solutions offers numerous advantages over traditional technologies (Akoh Atadoga et al., 2024). Patients can own, access, manage, and share their healthcare data, eliminating barriers associated with retrieving or transferring medical records across providers (Lu, 2018). Storing clinical information on a public, decentralized blockchain removes third-party dependency and enhances privacy and security by avoiding any single point of control. Despite these significant benefits and the growing potential of blockchain for Electronic Health Records (EHR), several critical challenges still persist. This paper analyzes these challenges in detail and proposes a comprehensive solution to overcome them.

Despite being immutable and highly fault-tolerant, the blockchain ledger is limited in its ability to store large data files based on images, documents, and video graphics (Casino et al., 2019). In the context, healthcare blockchain transactions would be comprised of actual factual events in terms of provided documentation and images associated with the healthcare services offered to patients (Shi et al., 2020). However, the decentralized distributed mechanism has a few drawbacks when storing big data generated by many users. Interoperability is still a huge problem in traditional systems because as long the data formats are heterogeneous and there is vendor lock-in it gets really difficult for data exchange, while blockchain has been proving that data exchange can be straightforward using standardized smart contracts (Carlos Ferreira et al., 2024). Furthermore, searching directly on encrypted data stored in a blockchain database is a desirable challenge, particularly in complex queries (Mawhayi et al., 2025) (Drew Ivan, 2016). To achieve patient privacy in a blockchain technology while performing search on encrypted data is also a key challenge. Searching for encrypted data in a ledger is inefficient and has privacy concerns. Therefore, efficient and reliable storage architecture and mechanisms are needed to ensure privacy, interoperability, efficient storage mechanism and efficient searching, which are the main focus of this research.

To address these challenges, we proposed a conceptual architecture that integrates encrypted cloud storage with a permission blockchain network, implemented using Hyperledger Fabric

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
and organized into specialized clusters to improve interoperability, storage efficiency, and privacy. The proposed architecture is mainly divided into N number of clusters based on *N* number of special category hospitals such as cancer, liver, cardiology, and oncology centers, as the number of users in a special hospital is relatively less than that of a general hospital, where the number is high and rich amount of data is being generated. The reason for these specified hospitals is to overcome the load of transactions which contain images and videos in a large volume of data in healthcare scenario. The aim is to provide scalable, reliable, and interoperable healthcare architecture using blockchain. The cloud is used as a backup mechanism to access the copy of data in the proposed architecture as well as for sharing data in the blockchain among different clusters used for solving the storage problem of blockchain. Moreover, to resolve the searching issue in a blockchain ledger we introduce "HealthSearchin" a privacy-preserving mechanism for efficient retrieval of patient records within the blockchain ledger. The "HealthSearchin" is a search mechanism, which incorporates a breadcrumb-based strategy to enable effective querying of encrypted healthcare data. While, in recent blockchain-based EHR system, for data retrieval in healthcare providers use either binary or keyword-based searching mechanisms, all of which are inefficient data searching (Liiv, 2021). Instead of binary or keyword-based searching we used a bread crumb indexing searching mechanism in the proposed system model to effectively use the searching of patients' healthcare data while also saving system computational time (Fan et al., 2018) (Lakshmi et al., 2024). In breadcrumb mechanism a directory of the summary of patient will be retrieved instead of whole ledger. Our proposed architecture emphasizes the fundamental requirements for the successful implementation of blockchain in healthcare, along with the key challenges associated with meeting these requirements.

The main contribution of this research article lies in proposing conceptual blockchain-based architecture for EHR that ensures secure and efficient data management. The architecture we proposed addressed major issues such as interoperability, storage constraints, searching in blockchain ledger, privacy and data loss in a single system architecture. By integrating blockchain with a cloud backup mechanism, the proposed model enables scalable, policy-driven, and cross-organizational data sharing while preserving confidentiality, integrity, and availability of sensitive medical information. Finally, searching for a patient record in a blockchain we proposed a "HealthSearchin" searching mechanism that is used bread crumb searching mechanism.

2. LITERATURE REVIEW

A wide range of studies have been explored blockchain-enabled e-healthcare from different perspectives, yet most solutions address only a subset of the challenges related to interoperability, privacy, ownership, searching and efficient data management.

The researcher in a study, (Drew Ivan, 2016) introduced a user-centric health data-sharing system using Hyperledger Fabric, emphasizing privacy through channel formation and membership services. Similar user-focused schemes were proposed by (Santos et al., 2021), who combined mobile data collection, cloud integration, and proof of integrity for secure health-data sharing. Interoperability remains a major challenge in healthcare. (Gordon and

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
Catalini, 2018) explored both institution-driven and patient-driven interoperability and suggested blockchain combined with cloud backup can enhance patient identity management, access control, data liquidity, aggregation, and immutability. The author in (Liang et al., 2018) proposed a scalable distributed blockchain architecture for large healthcare datasets, while (Zhang et al., 2017) introduced DApps to address fragmented records and communication gaps. DApps provide strong fundamental and structural interoperability, however they face difficulties with semantic interoperability because the storage and computation costs are high. MedBlock (Fan et al., 2018) and MedBChain (Al Omar et al., 2017) introduced architectures that focused on secure sharing of EMRs providing strong privacy assurances. MedBlock uses breadcrumb searching for efficient information mining, and MedBChain applies elliptic curve cryptography to obtain the pseudonymity in decentralized networks. Similarly, (Azaria et al., 2016) presented MedRec to support decentralized EMR management for tamperproof logging and patient access control to enhance confidentiality and interoperability. Also, in the article from (Kleinaki et al., 2018) utilized zero-knowledge proof for healthcare interoperability over blockchain. Likewise, the authors in (Xia et al., 2017) introduced MeDShare for secure sharing of medical data organized on smart contracts to facilitate auditing, provenance, and compromising access. Moreover, the article published by (Yue et al., 2016) designed the Healthcare Data Gateway (HDG), introducing purpose-centric access control and unified indexing to organize diverse medical data while using multiparty computation for privacy-preserving processing.

Distributed Archetypes Distributed systems development using archetypes (e.g., omniPHR) provided single holistic view of patient's medical record across different healthcare providers translating into better interoperability and increased patient engagement. In (Matthews & Coffrell, 2000) the authors presented PingER which benefited from permissioned blockchain with off-chain distributed storage to provide higher accessibility and performance. A few works combined blockchain with IoT and smart applications. Derived from the study of (Hang & Kim, 2019) proposed a block-chain-based IoT platform with ensuring secure data exchange, Identity management and real time monitoring. The work in (Zhao et al., 2017) utilized body sensor networks with blockchain for key recovery and secure data backup. In one study (Yin et al., 2021), the author proposed an incremental data updating for intelligent vehicle system. The author in a (Simic et al., 2017) integrated IoT and blockchain with big-data tools to ensure safety transfer of real time sensor data. Several works targeted security and cryptographic enhancements. An attribute-based signature scheme with multiple authorities and central authority in (Guo et al., 2018) was proposed by a researcher. Likewise, in (Ren et al., 2019), proposed a blockchain assisted storage system for Wireless Body Area Networks based on sequential aggregate signature to achieve storage saving and integrity property. Similarly, (Li et al., 2018) proposed blockchain-based data-preserving method to store verifiable medical data but secure the sensitive contents using cryptographic techniques.

Broader surveys e.g., (Agbo et al., & McGhin et al., 2019) described the potential of blockchain for applications like medical research, identity management, fraud detection and mobile health applications while also paying attention to shortcomings such as standardization issues, scalability problems and privacy leakage. (Wang et al., 2018) utilized parallel healthcare systems (PHS) and a consortium blockchain to improve diagnosis accuracy and decision

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
making by means of ACP (artificial societies, computational experiments, and parallel execution). Some other works are (Zyskind et al., 2015) which turned the blockchain into a decentralized access control manager that guarantees real data ownership, and (Cheng et al., 2018) in which they proposed a UPID to reduce linking errors among several hospitals. Also, the work by (Peelam et al., 2024) proposes decentralized blockchain based Cosmos network that addresses scalability and interoperability limitations in a blockchain system. It employs the Tendermint consensus and Inter-Blockchain Communication (IBC) protocol to ensure fast cross-chain transactions between chains across blocks. The Atom token from the network holds an important role in securing and governing it, also improving cross-chain communication.

In conclusion, the literature demonstrates the strong potential of blockchain to improve interoperability, data storage, searching in encrypted ledger, and security and privacy in e-healthcare. However, existing solutions tend to solve only one or two challenges in a single system architecture rather than addressing all key issues within a single unified architecture. This gap highlights the need for an integrated system capable of handling these challenges simultaneously.

3. PROPOSED METHODOLOGY

3.1.Perquisites

These experiments all run on the local system which has 4GHz, 4cores DELL 7 CPU with Hyperledger Fabric version 2.0. The system is built in hyperledger fabric, it is open-source distributed ledger technology built by IBM. Every node is running on isolated docker container. As blockchain is decentralized mechanism and used for secure transfer of assets between peers. So, we have taken advantage of this decentralized mechanism to secure the patients data across the healthcare system network. There are several prerequisites for hyper ledger fabric illustrated in *Table 1.*

Table 1: Prerequisites for Hyperledger fabric

Tools	Description
JDK 11.0	JDK includes tools used for development and testing of java programs
Hyperledger Fabric 2.0	It is a framework for developing permission blockchain network
Docker	It is a tool that deploy and run application in containerized environment
Go programming language	Used by component of hyper ledger fabric for network creation
Python	Used by component of hyper ledger fabric for network creation
Node Package Manager	Used by component of hyper ledger fabric for network creation
Curl	Curl tool can transfer data across the network by using various network protocol

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.2.Transaction flow of EHR management system

The transaction flow diagram illustrates in *Figure 1*, how healthcare data moves within the proposed blockchain-based system. Each cluster (Cluster A, B, and N) includes multiple healthcare entities such as specialized hospitals, pharmacies, and administrators. These entities generate transactions; for example, patient updates, medical records, or medication data; which are sent to the central "Anchor Peer." The Anchor Peer forwards the transactions to the Certification Authority (CA) for identity verification and access validation. Once authenticated, the transaction is processed through the Hyperledger Fabric network, where smart contracts handle data logic and commit the records to the appropriate blockchain channel. Finally, the validated blocks are distributed across all relevant peers, ensuring secure, consistent, and decentralized storage within each cluster.

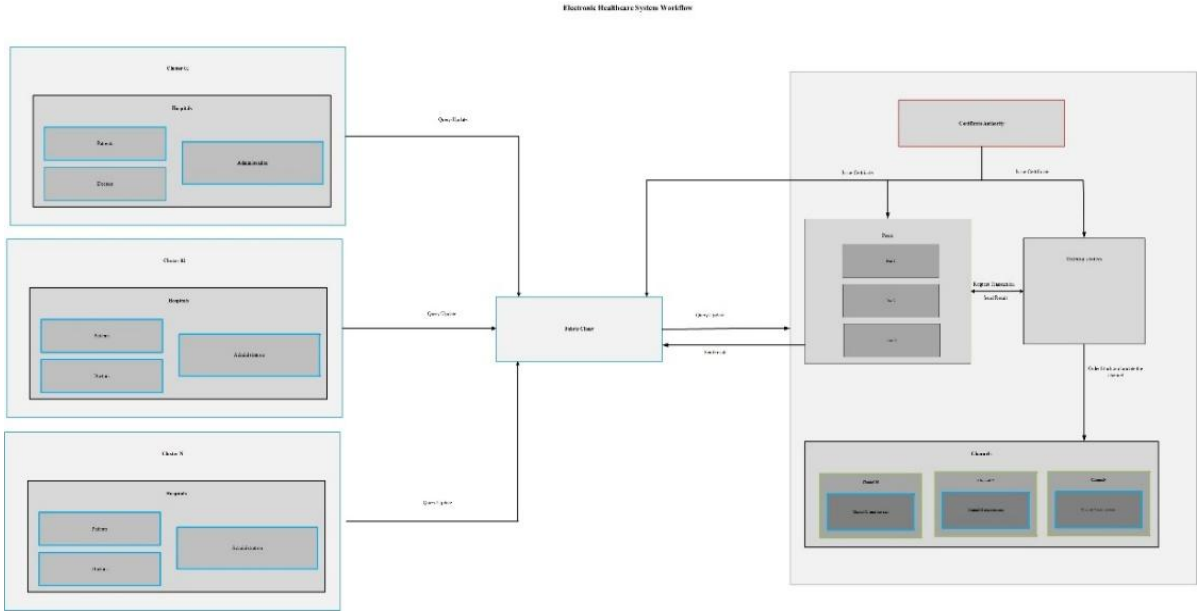

Figure 1: Transaction Flow of HealthCare system

3.3.Conceptual Architecture and Core Methodology

The proposed architecture of the healthcare blockchain model also overcome limitations of original databases storage by using cloud storage as elastic backup and interoperability means. Cloud storage provides anytime, anywhere access to shared resources and information with minimal administration of data replication for super-fluoride. The system is built on top of special service hospitals (cancer hospitals, liver and cardiology centers, trauma center, psychiatric hospital and oncology-facility) which are clustered the way they could have moderate size of data set load per cluster but high number of users in general all together-a mild balance solution. To further reduce these computationally expensive operations (instead of downloading an entire ledger or sending all the data to a client), we introduce an authorized breadcrumb searching approach, which makes it possible, for instance, patients' encrypted health summary split based on hospital department where they have attended and used collected data location as classification criteria (see *Figure 2*). Privacy and security are maintained with encryption and access control mechanisms.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

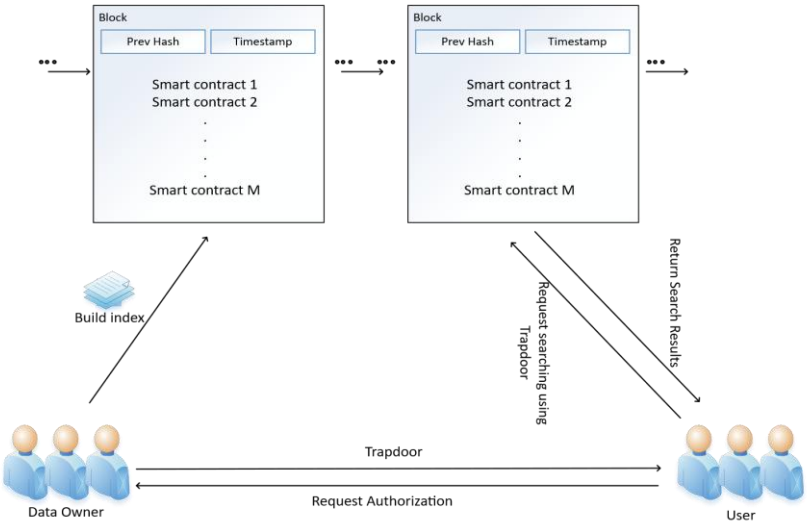

Figure 2: Searching for a mechanism in blockchain

The proposed architecture is 3-tier based with the organization layer responsible for city-wise hospital blockchains; Blockchain, which groups together hospital data on an aggregated ledger; and Storage to local cloud servers as backup and cross-organization sharing layered out in *Figure **3***. Blockchain Security: With cloud flaring the blockchain, all certified blocks are securely copied, speeding execution and interoperability for clusters and organizations. Data sharing is regulated by established policies and maintains the confidentiality of data as well as its integrity while allowing regulated access to government agencies, research institutions, and pharmaceutical companies. Through cloud's computational strength and elasticity, the model enables cost-effective decentralized interoperability, reduces risks of data loss, and allows for secure collaboration between healthcare providers and governmental institutions. Finally, the architecture offers an extendible, secure and privacy preserving solution to handle large-scale healthcare data including special organizations that hold sensitive information.

Since government authorities are also participants, only limited and non-sensitive patient information is maintained within it. These authorities do not query records using patient identifiers; instead, they retrieve data through specialized keyword-based searches (breadcrumb mechanism); such as disease names, hospital identifiers, or treatment categories. The detailed algorithm for the indexing breadcrumb retrieval process is presented in *Table 3*. Similarly, patients can access their own records see the details in *Table **2***, enabling them to review medication histories, recent diagnostic results, and other permitted clinical information, as illustrated in *Figure 2*.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

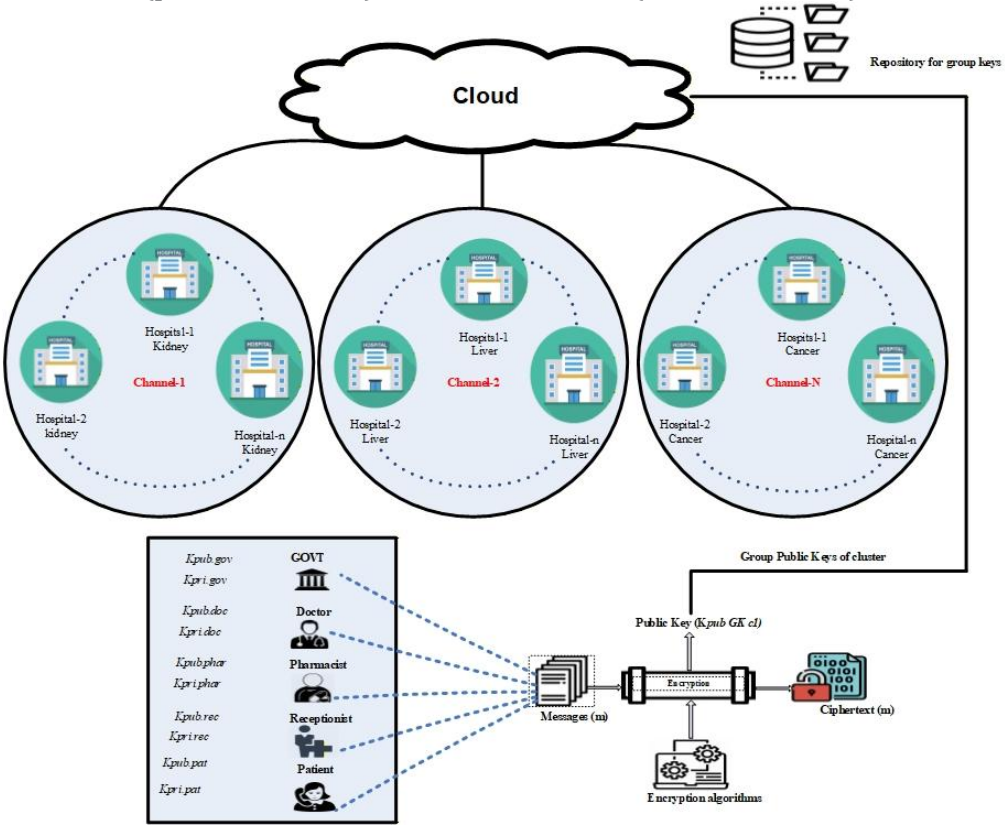

Figure 3: Searching mechanism in blockchain along with the cloud module

3.4. Implementation details

As mentioned previously we have divided our network into cluster. To implement the system, we make three cluster A, B and C. Hospitals in Cluster A are curing Cancer disease, Hospitals in Cluster B are curing kidney disease and Cluster C contains the government authorities that check, manage and audit health care issues. Each cluster contains the two hospitals that are curing the same disease, the endorsing hospitals of the cluster is shown in *Figure 4*.

```
faiza-aurangzeb@faizaaurangzeb-Inspiron-5406-2n1:~$ export MICROFAB_CONFIG='
{"port": 8080,
"endorsing_organizations":
  [
  { "name": "cancerhospitala"},
  { "name": "cancerhospitalb"},
  { "name": "kidneyhospitala"},
  { "name": "kidneyhospitalb"},
  { "name":  "governmentorg" }
  ],
```

Figure 4: Clusters having hospitals.

As we all know, in hyper ledger fabric not only endorsing organizations are involved but there are many other many entities like channels, smart contracts and chaincode.

3.5. Smart contract

Smart contract defines the business rules through which communication takes place on channels we have created three channels in our healthcare system and for each channel we have

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
defined separate business rules for communication and make three smart contracts the detail of each smart contract is described below.

- Administrator can view the patients' details.
- Administrators can update contact info and address of patients.

The roles of doctor on this channel are the following:

- Doctors can update the medication information of patient based on patient key.
- Doctor can update the Disease information of patient based on patient key.
- Doctor can update the checkup results of patient based on patient key.

Table 2: Algorithm 1 for registration of patient

Algorithm 1: Register Patient

Input: Patient Info
Output: Registration successful
Require: Patient Id, Name, Address, and Contact Info

1. Register Patient: (ctx, Patient Id)
2. **If** Patient Id exists on network, **then**
3. alert patient already exists
4. **Else if** Patient Id does not exist on network **then**
5. Convert the patient data into Json format
6. Insert the patient data in CouchDB along with patient Id
7. **End**

Table 3: Algorithm 2 for Search patient through breadcrumb mechanism

Algorithm 2: Breadcrumb Search for Patient EMRs

Input: List of keywords Output: Display matched patient EMR summaries
Require: Hospital department, location metadata

8. Initialize context: ctx ← getPatientContext(keywords)
9. Identify cluster: cluster ← locateCluster(ctx.department, ctx.location)
10. Access breadcrumb index: breadcrumb ← fetchBreadcrumb(cluster, keywords)
11. **If** breadcrumb.size > 0 then
    a. data ← retrieveEncryptedSummaries(breadcrumb)
    b. jsonData ← convertToJSON(data)
    c. display(jsonData)
12. **Else** alert ("No matching patient information found for the given keywords.")
13. **End**

3.6. Cloud Module

In our proposed architecture in *Figure 3*, the cloud serves exclusively as a backup and accessibility mechanism for replicated data. Integrating a cloud database improves the execution speed of operations involving blockchain ledgers and significantly enhances interoperability across blockchain clusters and external organizations. It also facilitates controlled cross-organizational access to necessary data stored in the cloud. All data-sharing

Received: August 06, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
operations follow predefined policies that specify the scope and granularity of information accessible to each requesting entity.

The cloud component enables scalable, on-demand access to shared computational resources with minimal administrative overhead. Its substantial computational capacity ensures reliable support for cross-organizational data requests. The cloud module is incorporated for two key purposes:

- To provide reliable data backup, enabling organizations to recover information in case of on-premises data loss.
- To support interoperability among healthcare institutions within or outside a cluster.

The cloud module is implemented using a XAMPP server. Whenever a transaction is generated at the hospital, the encrypted data is simultaneously synchronized to the cloud server. In the event that any hospital loses its local data, it can seamlessly restore it from the cloud.

4. RESULTS AND DISCUSSION

This section discussed the results of our implementation. In this article, we presented a conceptual single system architecture to overcome these limitations, including interoperability, storage space limitation and searching in blockchain ledger etc. By employing encrypted cloud for data storage referred by the permissioned blockchain network (gather from open sources) constructed with Hyperledger Fabric and organized into proprietary clusters of specialized consortiums enhance scalability and privacy.

The results show that the technique is efficient in query performance with growing numbers of matched documents. As can be seen in the figure, the search time slowly ramps up from about 3ms to 24ms when the number of found documents go from 50-1200. This almost-linear scaling demonstrates that the breadcrumb mechanism is indeed successful in cutting down the required full-ledger scanning, by reducing our search space to relevant indexed entries. In totality, the method has achieved high performance efficiency and thus it is appropriate for encrypted healthcare big data systems. The results of breadcrumb records are shown in *Figure 5*.

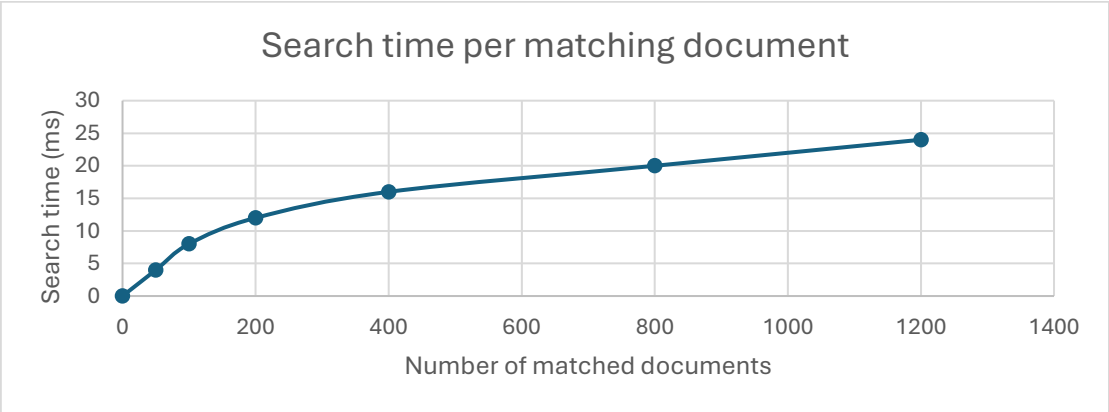

Figure 5: Search Time per matching document

In the proposed healthcare system, patients are registered exclusively by the hospital administrator. Once registered, a patient can perform various transactions on the network, such as viewing medical records and accessing medication information. Multiple patients have been

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
registered in our system, and the average block creation time is approximately 20ms. *Figure 6* illustrates the block creation process for the first three registered patients.

```
[11/30/2022 12:49:51 PM] [INFO] submitting transaction createPatient with args 1235,fizza,atd,
0303,cancer,nill,suliman,12/06/2022,ok,A on channel cancerpatientinfo to peers
cancerhospitalbpeer-api.127-0-0-1.nip.io:8080,cancerhospitalapeer-api.127-0-0-1.nip.io:8080
[11/30/2022 12:49:51 PM] [SUCCESS] No value returned from createPatient
[11/30/2022 12:52:09 PM] [INFO] Open Transaction View
[11/30/2022 12:52:35 PM] [INFO] submitTransaction
[11/30/2022 12:52:35 PM] [INFO] submitting transaction createPatient with args 1236,fizza,atd,
0303,cancer,nill,suliman,12/06/2022,ok,B on channel cancerpatientinfo to peers
cancerhospitalbpeer-api.127-0-0-1.nip.io:8080,cancerhospitalapeer-api.127-0-0-1.nip.io:8080
[11/30/2022 12:52:35 PM] [SUCCESS] No value returned from createPatient
[11/30/2022 12:53:31 PM] [INFO] Open Transaction View
[11/30/2022 12:53:48 PM] [INFO] submitTransaction
[11/30/2022 12:53:48 PM] [INFO] submitting transaction createPatient with args 1237,fizza,atd,
0303,cancer,nill,suliman,12/06/2022,ok,B on channel cancerpatientinfo to peers
cancerhospitalbpeer-api.127-0-0-1.nip.io:8080,cancerhospitalapeer-api.127-0-0-1.nip.io:8080
[11/30/2022 12:53:49 PM] [SUCCESS] No value returned from createPatient
```

Figure 6: Shows the time for the block creation of first three patients.

To evaluate the performance of the proposed system, we simulated multiple organizations and generated many medical records. The execution time for modify and query operations differs because a modify transaction inserts new data into the ledger, whereas a query transaction only retrieves existing information. Therefore, both create and read transactions were utilized to assess the system's performance. First, we employed the create transaction defined in the patient smart contract to generate medical records. As a patient client, we then issued an increasing number of concurrent modify requests through the Fabric clients until the network reached saturation, enabling us to determine the maximum throughput in terms of modify transactions per second. Subsequently, to measure the saturated throughput for read queries, we submitted progressively increasing query requests against the previously generated medical records.

The performance of a blockchain can be impacted by a number of factors, including the operating environment, transaction size, number of endorsing nodes, and block size. Because the environment, transaction size, and number of endorsing nodes are all constant in our experiment, we chose block size as a configuration parameter to evaluate how it affects the performance and latency of our system.

In this proposed solution, we used Hyperledger Caliper to measure the system's results and chose four distinct block sizes: 0.5MB, 1MB, 1.5MB, and 3MB. We can observe in *Figure 7* that the value of transactions per second is going to saturate at 1MB block size. The value of transactions per second barely grew marginally beyond 1MB. And the value of create transactions per second is lower than read, since create transactions transaction sizes are bigger than read transactions. As a result, transit takes longer.

The link between network latency and block size is depicted in *Figure **8***. When the block size is increased, the network's latency increases dramatically. The reason for this is that ordering transactions and aggregating them to the block will take longer with a larger block. As a result, the 1MB block size may be the best option for our network. VISA processes around 2000 transactions per second, while our system processes around 600.

Received: August 06, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

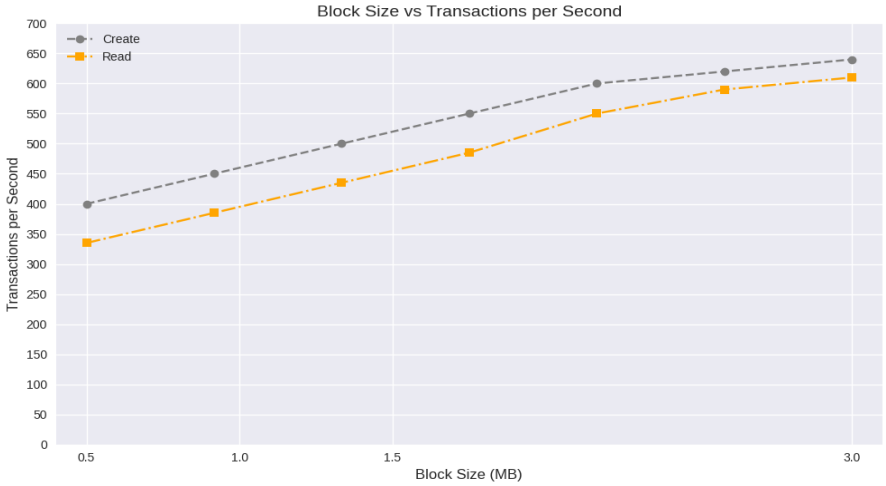

Figure 7: Throughput of created and read transaction

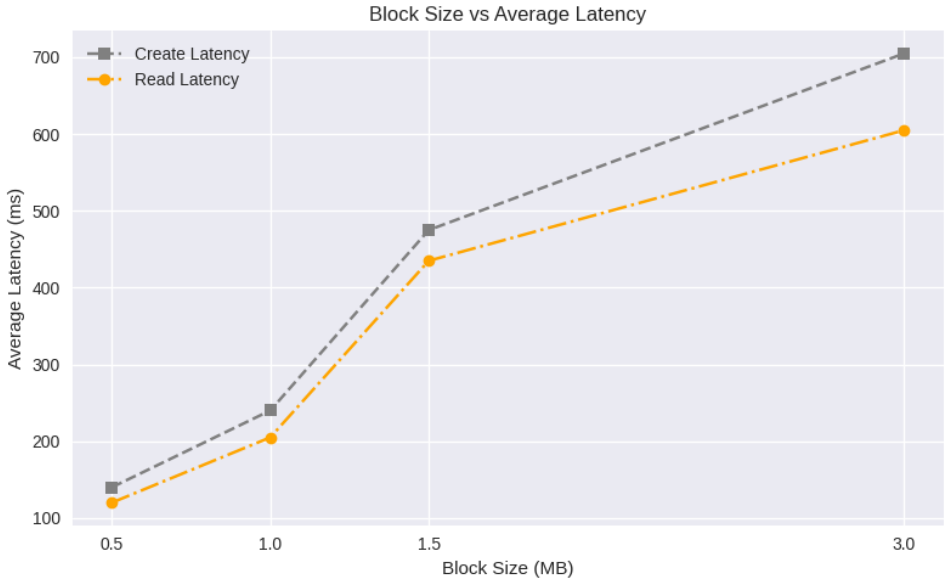

Figure 8: Average latency of read and created transactions

5. CONCLUSION AND FUTURE WORK

In conclusion, the context of a smart healthcare environment, we have designed, built, and assessed "HealthSearchin" framework and end-to-end secure data sharing architecture based on blockchain technology. The proposed system uses blockchain and cloud to guarantee the sharing of health data among various stakeholders. Additionally, it employs a cutting-edge Privacy Agreement Management Scheme that keeps track of how well the service is being delivered in accordance with patient wishes and privacy rules. It also involves efficient searching mechanisms using breadcrumb which provides both user level and data level privacy. The proposed architecture is practical and effective for healthcare contexts in terms of storage, interoperability, and searching, according to security analysis and testing results.

REFERENCES

[1] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
healthcare: A systematic review. *Healthcare (Switzerland)*, *7*(2). https://doi.org/10.3390/healthcare7020056

[2] Atadoga, A., Elufioye, O. A., Omaghomi, T. T., Akomolafe, O., Odilibe, I. P., & Owolabi, O. R. (2024). Blockchain in healthcare: A comprehensive review of applications and security concerns. *International Journal of Science and Research Archive*, *11*(1), 1605-1613.

[3] Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). MediBchain: A blockchain based privacy preserving platform for healthcare data. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10658 LNCS*, 534–543. https://doi.org/10.1007/978-3-319-72395-2_49

[4] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 25–30. https://doi.org/10.1109/OBD.2016.11

[5] Carlos Ferreira, J., Elvas, L. B., Correia, R., & Mascarenhas, M. (2024, October). Enhancing EHR interoperability and security through distributed ledger technology: A review. In Healthcare (Vol. 12, No. 19, p. 1967). MDPI.

[6] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36(November 2018), 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[7] Cheng, E. C., Le, Y., Zhou, J., & Lu, Y. (2018). Healthcare services across China–on implementing an extensible universally unique patient identifier system. International Journal of Healthcare Management, 11(3), 210–216. https://doi.org/10.1080/20479700.2017.1398388

[8] Drew Ivan. (2016). Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. ONC/NIST Use of Blockchain for Healthcare and Research Workshop, August, 11.

[9] Gavrilov, G., Jakimovski, B., Chorbev, I., & Trajkovik, V. (2018). Cloud-Based Electronic Health Record for Health Data Exchange. October, 11–16. https://doi.org/10.20544/aiit2018.p03

[10] Lakshmi, S. M., Malathi, M., & Mythili, K. (2024). Blockchain-enabled security for smart medicine vending machines handling expired medications. Blockchain-Enabled Solutions for the Pharmaceutical Industry, 189-206. https://doi.org/10.1002/9781394287970.ch10

[11] Lu, Y. (2018). Blockchain and the related issues : a review of current research topics. Journal of Management Analytics, 0(0), 1–25. https://doi.org/10.1080/23270012.2018.1516523

[12] Peelam, M. S., Chaurasia, B. K., Sharma, A. K., Chamola, V., & Sikdar, B. (2024). Unlocking the potential of interconnected blockchains: A comprehensive study of cosmos blockchain interoperability. *IEEE Access*.

[13] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of Medical Systems, 40(10). https://doi.org/10.1007/s10916-016-0574-6

[14] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
assessing blockchain-based healthcare decentralized apps. 2017 IEEE 19th International Conference on E-Health Networking, Applications and Services, Healthcom 2017, 2017-Decem, 1–4. https://doi.org/10.1109/HealthCom.2017.8210842

[15] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Received: August 06, 2025