

Blockchain System for Trustless Healthcare Data Sharing with Hyperledger Fabric in Action

Muhammad Mohsan Sheeraz
*Institute of Digital Anti-Aging
Healthcare*
Inje University
Gimhae, South Korea
sherazmohsin257@gmail.com

Md Ariful Islam Mozumder
*Institute of Digital Anti-Aging
Healthcare*
Inje University
Gimhae, South Korea
arifulislamro@gmail.com

Muhammad Omair Khan
*Department of Computer Science
Islamia College Peshawar*
Peshawar, Pakistan
mumairkhan690@gmail.com

Muhammad Usama Abid
*Institute of Digital Anti-Aging
Healthcare*
Inje University
Gimhae, South Korea
usamamughal735@gmail.com

Moon-ill Joo
*Institute of Digital Anti-Aging
Healthcare*
Inje University
Gimhae, South Korea
joomi@inje.ac.kr

Hee-Cheol Kim
*College of AI Convergence / Institute of
Digital Anti-Aging Healthcare*
Inje University
Gimhae, South Korea
heeki@inje.ac.kr

Abstract— Healthcare data security is a much-discussed topic nowadays. Medical data storage and sharing require security, privacy, and trust between organizations. Different research organizations, medical institutes, or individual researchers publish their research results but sometimes they need to share the data as well. In this scenario, a secure and transparent medical data-sharing system is much needed. In this work, we are proposing a blockchain-based system for medical data sharing between organizations. The system ensures security, privacy, transparency, and trust, hence trust between the organizations is not necessary. Since the system requirement is permissioned, a private or permissioned blockchain is used. We have set up the blockchain infrastructure using hyperledger fabric, known for its flexibility and modular architecture.

Keywords— *medical data, medical image, security, privacy, data sharing, blockchain, hyperledger fabric*

I. INTRODUCTION

Twenty years ago, any medical images that originated in digital form were printed to film or otherwise rendered analog, and radiographs were housed in jacketed folders in a film library. There was room for privacy breaches but not nearly on the scale possible today. Today, medical images are digitized, stored, sent, and downloaded in a variety of scenarios. we are facing a new era of unique scientific challenges regarding medical data handling and patient privacy [1]. A consistent approach to protecting patient information is needed to take care of the patient's privacy interests [2].

Researchers and organizations involved in medical research are require medical data to satisfy their requirements or to publicize the original data with the presentation of their research work. Medical data can be shared with a limited number of researchers or organizations to perform analysis but not possible to share with a large number of researchers or interested organizations. One of the main problems is government regulations in most countries for example in the United States the HIPAA act (Health Insurance Portability and Accountability Act) [4], the Convention for the Protection of Individuals concerning the Automatic Processing of Personal Data in Europe [5] forbid the sharing of health information (PHI) and at the same time do not provide the software or mechanism that can be followed to share the data according to the regulations. An

organization might be sharing the data with other organizations if they had a business relationship, however, this depends on the data center or its institutional review board (IRB) whether permit the sharing of data or not.

The imaging center staff may be aware of the rules and regulations but they may not have the proper tools and expertise to de-identify the data before it will be shared for publication. The organization or research center that needs this data may have imaging data de-identification software, but the imaging center is still responsible and have legal liability.

Blockchain is a peer-to-peer decentralized technology that is used in several domains such as financial applications, supply chains, healthcare, etc [6,7]. Blockchain technology provides a secured distributed database, that prevents any unauthorized access to stored data [8]. It is a highly suitable infrastructure solution in the case of sharing data between multiple parties. Blockchain systems are cost-effective and also require very less maintenance over a long time, at the same time these systems are very efficient [9, 10].

InterPlanetary file system (IPFS) is a decentralized, peer-to-peer file storage system [11]. Data uploaded to the IPFS is available within the network, any peer can request the data. Data stored on IPFS is assigned a unique has, that is the address of that data in the network.

II. RELATED WORK

Xia et al. [12] raised a system for preserving data privacy utilizing blockchain technology. In this study, the authors proposed a permissioned blockchain system that grants knowledge to the data kept in the cloud repository, allowing access to data requests. They used the data grantors, who permit the collection and analysis of data that results in value derivation. Their experimental research proved the system's flexibility, scalability, and lightweight. The Healthcare data gateways (HDG) system is a decentralized blockchain-based risk-control system, worked by Xiao Yue et al. [13]. In this system, Patient data confidentiality is maintained as a new latent approach to enhancing healthcare systems is presented by the patient's ability to securely own, control, and disseminate his data. According to HDG results, this system is trustworthy and auditable since it uses a decentralized network of peers, which is performed using a public ledger. Azaria et al. [14] developed the first and only solution

offered and used some smart contracts to assign the proper rights for private data sharing in the MedRec medical record-sharing prototype. The first and only solution offered used some smart contracts to assign the proper rights for private data sharing in the MedRec medical record-sharing prototype. MedRec offers records that are flexible and fine-grained, which encourages health data reviewers to keep the network up and simplifies the interchange of patient data. In this study, the researchers used a ledger to keep track of patients, healthcare practitioners, and researcher contacts in a way that could be audited. Ichikawa et al. [15] proposed a tamper-resistant mHealth policy based on blockchain methodology, which provides observable computing and reliable policies. They proposed a mHealth network system in this system for cognitive-behavioral treatment of somnolence ("sleepiness") sickness by creating a smartphone app. Additionally, they voluntarily obtained the Electronic Medical Records (EMR) from the patients via the app and saved them in JSON format, which was then successfully transferred to the Hyperledger Fabric permissioned blockchain network. The tamper resistance of the EMRs produced by fake faults was next examined by the authors. The combination of mHealth and blockchain Hyperledger Fabric may offer a novel explanation that empowers approachability and data clarity without using a third party.

A data-sharing scheme dependent on the blockchain has been used by Hussein [16] for addressing the matters of access control with blockchain technology, such as immutability and autonomy features. In this study, the researcher used an interesting genetic algorithm and a discrete wavelet transform (DWT) to improve the queuing optimization method. As a result, it creates a cryptographic key to provide access control and immunity, enabling quick user authentication. Dagher et al. [17] proposed a blockchain-based approach for delivering secure, interoperable, and dynamic access to medical records while preserving sensitive patient data. Therefore, to provide access control and data obfuscation, researchers used the Ethereum blockchain in this system. They also deployed cryptographic techniques for added security. Chen et al. [18] architected a storage system to maintain blockchain technology-based individual medical cloud and data storage. They use blockchain technology to create a storage supply chain in which all transactions are traceable, responsible, and verifiable.

The main purpose of the medical blockchain was composed of this system, which also established the rights for three different kinds of transactions. They also developed a service framework for sharing medical records that safeguard apps for managing medical data while abiding by privacy laws. Zhang et al. [19] proposed a personal health information-sharing protocol for the Blockchain-based e-Health system that is safe and protects privacy and is used to improve diagnosis. Additionally, they discussed the blockchain consensus method, which was designed to create confirmed blocks and serve as proof of compliance. Additionally, researchers used public-key encryption with a blockchain-based keyword search. After receiving information from the patient, a doctor is permitted to search and examine the anticipated history of health records to improve the diagnosis. They asserted that this electronic health record system provides confidentiality, privacy preservation, and secure medical data search.

III. PROPOSED SYSTEM

A. Scenario

Medical image data sharing between different organizations is a tough topic. It is important to have a system that facilitates data sharing in a trusted environment, and stores the data and related information for later use. In this system, A Hyperledger Fabric architecture is designed in a scalable manner, initially, there is a consortium of three organizations but in the future new organizations can be added easily just by running a few scripts. Every organization registers admin users by using certificates issued by the certification authority. Then these users access the system by using admin user credentials. Every admin user has access to upload the data and all of the uploaded data. The admin user also has some restrictions such as only the data owner organization's admin can delete the data and the rest of the organization's admins have access to only download the data but cannot delete it. Once a data file is uploaded it will remain available in the file system and can be downloaded at any time until the owner organization deletes it.

B. Admin User Use Case

Every participating organization has an admin user that interacts with the system. As shown in fig. 1 the admin user can perform various operations such as data uploading, view & download the shared data and manage own data. The admin user uses login credentials to interact with the system.

C. Architecture

The high-level system architecture is defined in fig. 2. Blockchain operator set up the network and the initial configurations, create the users, and provide them with the necessary information and credential to access and govern the network. All the peers are representing fabric peer, orderer, and ca images, these entities are hosted in docker containers. The Hyperledger fabric peers are hosting ledger and chaincodes. Each peer is related to its corresponding hospital by the same color. The backend framework is Nodejs, code is written in Javascript and Expressjs is used to write the REST API's. The fabric SDK provides support for various programming languages such as Java, Go, and Javascript. These SDKs are used for communication between the backend and fabric network. In this system Fabric SDK for Nodejs is used. The front end is developed using Angular Framework, which provides structured components to develop an interactive user interface. The communication between both components is enabled through REST API calls and the JSON web tokens are used for authentication.

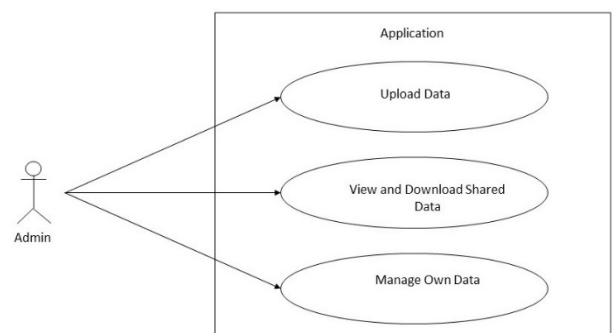


Fig. 1. Admin user use-case

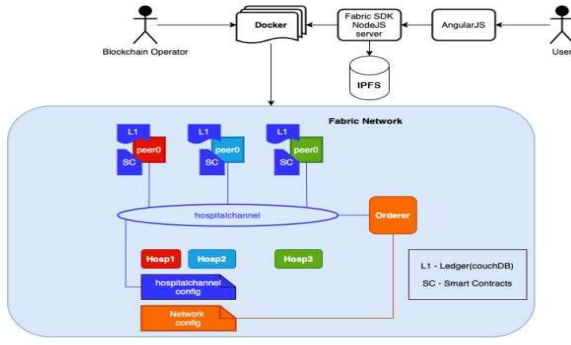


Fig. 2. System architecture

According to the scenario the “hospitalChannel” is created and joined by the three hospital organizations. Since the system architecture is scalable, so the new organization can be added anytime.

Hyperledger Fabric supports two types of peer databases, CouchDB and LevelDB. CouchDB is a NoSQL database, that uses JSON to store the data and provides javascript-based querying capabilities. The CouchDB is an optional or alternative state database and is used in this solution because of its JSON query capability and flexibility. The LevelDB is the default state database that is embedded with the peer binary, stores data in the key-value format, and only supports key, key range, and composite key queries. Both databases could be used to store the ledger data, which contains transaction logs and world state. In this system, CouchDB is used to store the world state, and LevelDB is used to store the transaction logs. As I stated earlier, every component of this system is pluggable, which could easily be removed or replaced.

D. System Workflow

Fig. 3 shows the process of uploading the medical data and record creation in the ledger. First, the admin made the connection request from the user interface to the nodejs server, the server does the authentication of the admin JSON web token, and after successful authentication, the connection request is forwarded to the network through the

Fabric SDK, upon receiving the request, the network checks the admin certs and establishes the connection. After the successful connection the admin uploads the data, the data first goes to the server, then uploaded to IPFS and a hash is returned that is the address of the data on IPFS.

Now the server forwards the transaction request to the network through the Fabric SDK along with the address hash and data owner information. The smart contract named DataStore is invoked and the record is created into the ledger.

The admin can download any existing data with just a single click. Admin requested downloading the data to the node server through REST API's. The server authenticates the admin JSON web token, after successful authentication, the server looks for the requested data from IPFS and sends the data back in response.

IV. CONCLUSION

In this research work, we have proposed a blockchain system using Hyperledger fabric, IPFS, Nodejs, and AngularJs technologies. The core purpose of the system is to facilitate medical organizations and research institutes to share medical data in a trustless environment. The proposed system ensures data privacy and availability with enhanced security. It provides restricted access to data with verifiable credentials. Blockchain makes this system transparent and retains the ownership of the data. Every data transaction is recorded in the ledger and can be used for audit purposes. Smart contracts are playing an important role in this system, ensuring fair data distribution and the enforcement of rules.

ACKNOWLEDGMENT

This work is supported by the Commercialization Promotion Agency for R&D Outcomes (COMPA) grant funded by the Korean Government (Ministry of Science and ICT) (R&D project No.1711139492)

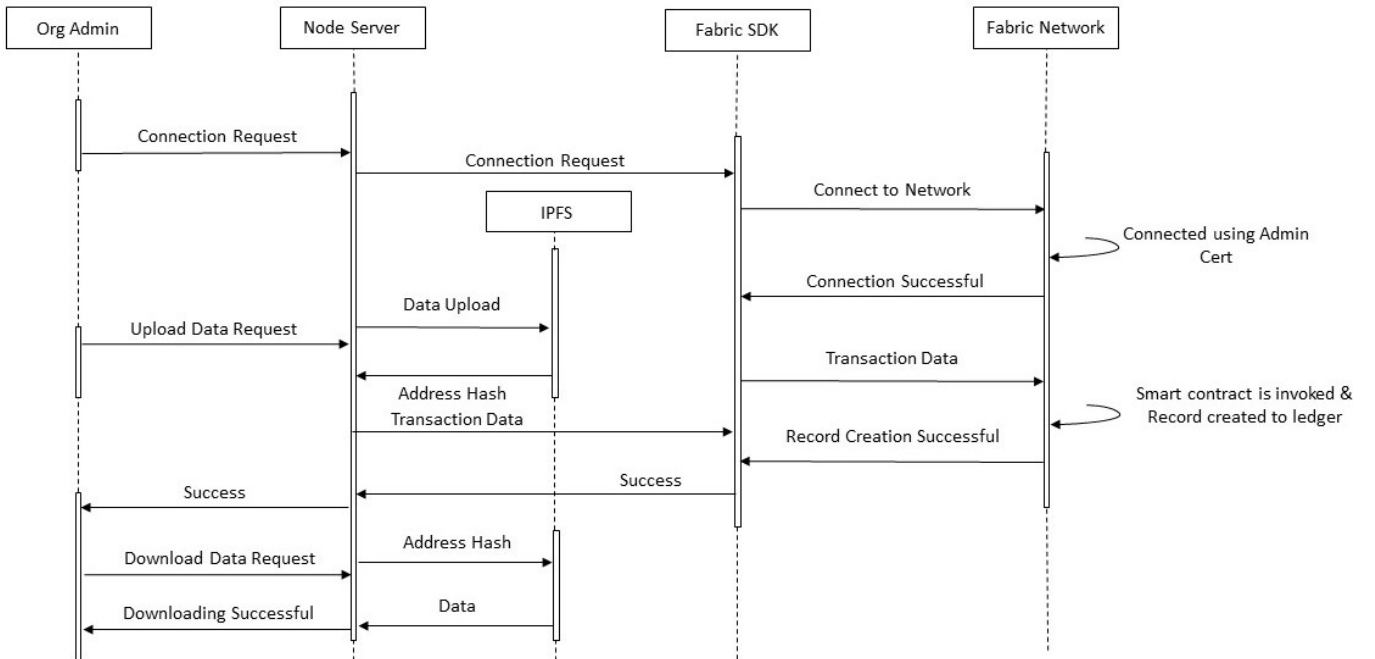


Fig. 3. System Workflow

REFERENCES

- [1] W. Nicholson, and I. Glenn Cohen. "Privacy in the age of medical big data." *Nature medicine* 25.1 (2019): 37-43.
- [2] Adams SJ, Tang R, Babyn P. Patient Perspectives and Priorities Regarding Artificial Intelligence in Radiology: Opportunities for Patient-Centered Radiology. *J Am Coll Radiol*. 2020 Aug;17(8):1034-1036. doi: 10.1016/j.jacr.2020.01.007. Epub 2020 Feb 14. PMID: 32068006.
- [3] Al Omar, Abdullah, et al. "Medibchain: A blockchain based privacy preserving platform for healthcare data." *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, Cham, 2017.
- [4] Annas, George J. "HIPAA regulations: a new era of medical-record privacy?." *New England Journal of Medicine* 348 (2003): 1486.
- [5] Levin, A., & Nicholson, M. J. (2005). Privacy law in the United States, the EU and Canada: the allure of the middle ground. *U. Ottawa L. & Tech. J.*, 2, 357.
- [6] Zile, K., & Strazdiņa, R. (2018). Blockchain use cases and their feasibility. *Applied Computer Systems*, 23(1), 12-20.
- [7] Zhang, Peng, Douglas C. Schmidt, Jules White, and Gunther Lenz. "Blockchain technology use cases in healthcare." In *Advances in computers*, vol. 111, pp. 1-41. Elsevier, 2018.
- [8] Peng, Zhe, Haotian Wu, Bin Xiao, and Songtao Guo. "VQL: Providing query efficiency and data authenticity in blockchain systems." In *2019 IEEE 35th international conference on data engineering workshops (ICDEW)*, pp. 1-6. IEEE, 2019.
- [9] Olsen, Petter, Melania Borit, and Shaheen Syed. "Applications, limitations, costs, and benefits related to the use of blockchain technology in the food industry." *Nofima rapportserie* (2019).
- [10] Benton, Morgan C., N. M. Radziwill, A. W. Purritano, and C. J. Gerhart. "Blockchain for Supply Chain: Improving Transparency and Efficiency Simultaneously." *Software Quality Professional* 20, no. 3 (2018).
- [11] Benton, Morgan C., N. M. Radziwill, A. W. Purritano, and C. J. Gerhart. "Blockchain for Supply Chain: Improving Transparency and Efficiency Simultaneously." *Software Quality Professional* 20, no. 3 (2018).
- [12] Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 8(2), 44.
- [13] Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." *Journal of medical systems* 40.10 (2016): 1-8.
- [14] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016.
- [15] Ichikawa, Daisuke, Makiko Kashiwayama, and Taro Ueno. "Tamper-resistant mobile health using blockchain technology." *JMIR mHealth and uHealth* 5.7 (2017): e7938.
- [16] Hussein, Ahmed F., et al. "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform." *Cognitive Systems Research* 52 (2018): 1-11.
- [17] Dagher, Gaby G., et al. "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology." *Sustainable cities and society* 39 (2018): 283-297.
- [18] Chen, Yi, et al. "Blockchain-based medical records secure storage and medical service framework." *Journal of medical systems* 43.1 (2019): 1-9.
- [19] Zhang, Aiqing, and Xiaodong Lin. "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain." *Journal of medical systems* 42.8 (2018): 1-18.