Pimpri Chinchwad Education Trust's

Pimpri Chinchwad College of Engineering, Pune

6th International Conference on Computing, Communication, Control and Automation (ICCUBEA-2022)

Presentation By: Vishaal Prasad, Harsh Wadhawe

PAPER ID : **82**

PAPER TITLE : Electronic Health Record Management using Hyperledger Fabric

Authors:

Harsh Wadhawe

Rohit Kota

Vishaal Prasad

Under Guidance of Prof. Rohini Sarode

- Introduction
- Problem Statement
- Objectives
- Literature Review
- Methodology
- Results
- Conclusion
- References (Selected)

Please Note :Authors may add points as per their research paper contents.

Introduction :

- Electronic Health Records (EHR) store and share medical data as Electronic Medical Records (EMRs), which contain a patient's medical diagnoses, allergies, history, treatment, lab reports etc.
- Ensuring data integrity, confidentiality and privacy of patients and clinical data and maintaining interoperability among entities is essential.
- Lack of client control over data can lead to unauthorized accessing/ editing of medical information.

Problem Statement :

- We propose a permissioned blockchain-based Patient Data Management system using Hyperledger Fabric (HLF), which allows patients to control their medical information and grant or revoke access to doctors for data.
- Ensures that all entities have a holistic view of transactions and interactions.

Objectives :

Why Blockchain and Hyperledger Fabric (HLF)?

- Authentication and authorization
- Confidentiality and availability
- Data integrity and privacy
- pBFT (Practical Byzantine Fault Tolerance) consensus algorithm

Literature Review :

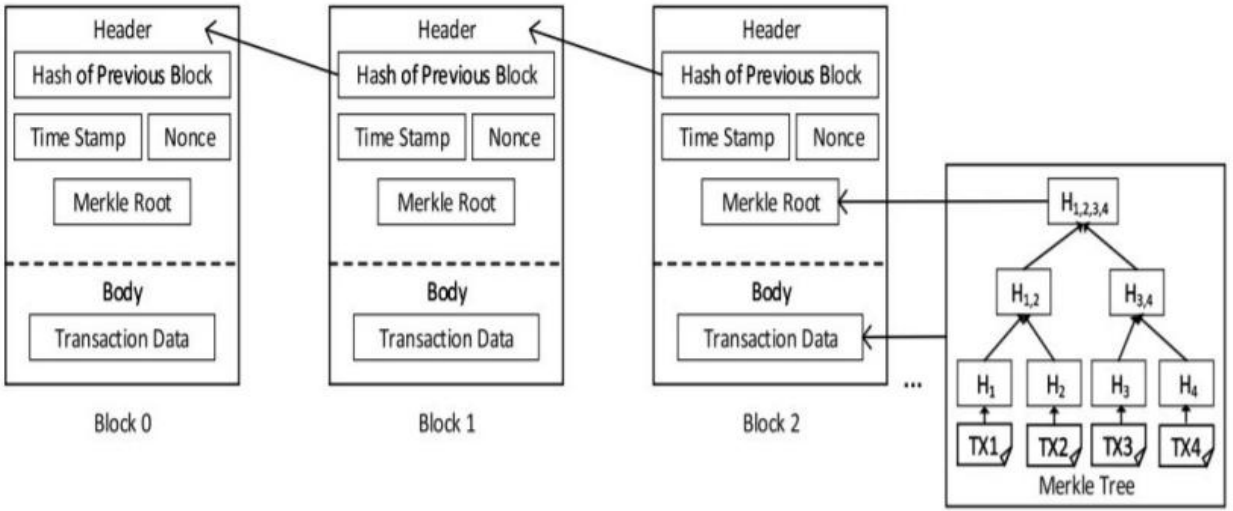
TITLE	SUMMARY
A Blockchain based Electronic Medical Health Records Framework using Smart Contracts	Blockchain allows ease of access to the records as it is available to any personnel authorized to access them. Adopting Blockchain to deploy EHR solves the issues of accessibility and authority.
Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric	Building EHRs based on the Hyperledger Fabric will ensure that patients have full access to their records, patient's data are stored securely and only verified participants can interact with patient's sensitive data.
Hyperledger fabric: a distributed operating system for permissioned blockchains	Fabric supports modular consensus protocols, allowing the system to be tailored to particular use cases and trust models.
Lightweight Blockchain for Healthcare	Experimental results demonstrated that their proposed architecture generated 11 times lower network traffic compared to the Bitcoin network as the number of blocks increased. Their ledger update was also 1.13 times faster.

Literature Review :

TITLE	SUMMARY
Blockchain Application with Health Token in Medical & Health Industrials	There are different types of blockchains for recording and tracking different types of processes, exchanging and providing information on each and every part of the population including digital health assets.
ETH Relay: A Cost - efficient Relay for Ethereum - based Blockchains	ETH Relay is able to reliably verify the inclusion of transactions across blockchains and does not require trust in a centralized party. Reduced the cost of operating a relay between Ethereum-based blockchain by 92%.
Based Private Blockchain (ICCIT)	Data is publicly available, it is not suitable for developing a secured forensic system.

What is Blockchain:

- Decentralized framework guaranteeing data integrity, security, and smart contracts for data access via a secure distributed database to make queries



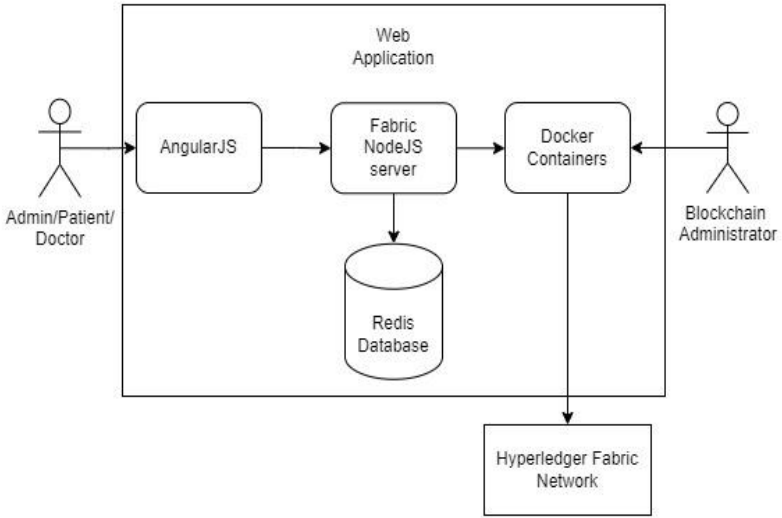
Introduction to Hyperledger Fabric:

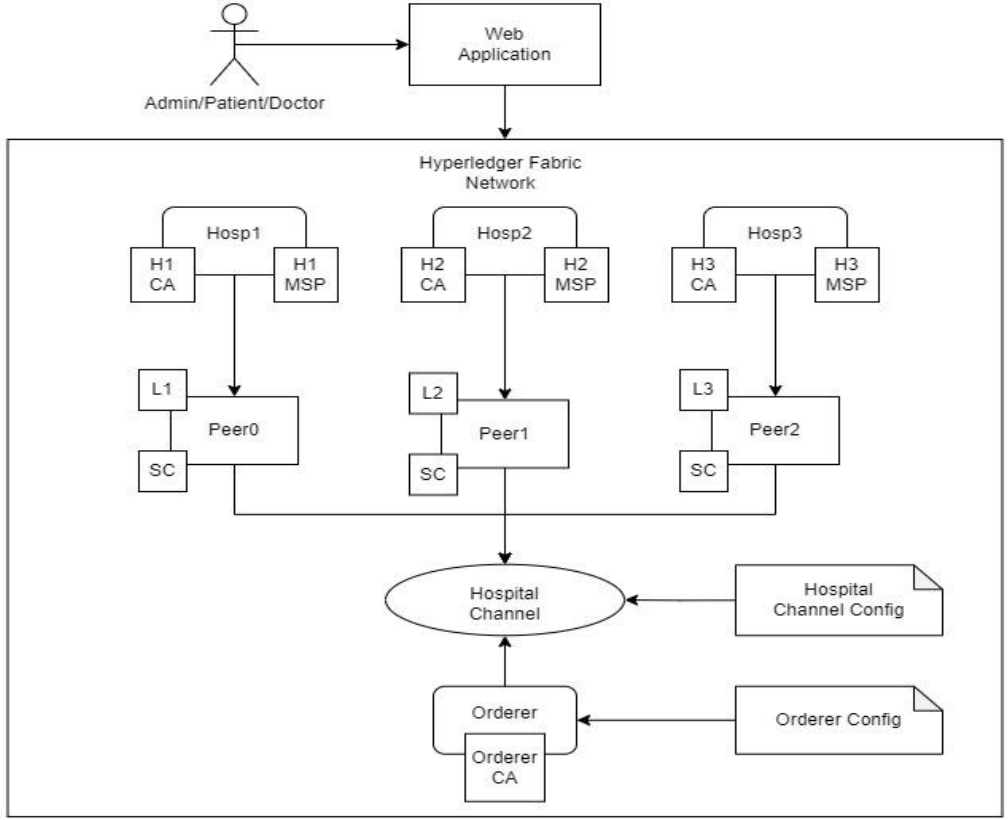
- A permissioned and private blockchain providing an immutable distributed ledger network to carry out transactions within the same network.

HLF components:

- Membership service provider (MSP) and Certificate Authority (CA)
- Distributed ledger
- Channel
- Smart Contract and Chaincode
- Identity
- Endorsement policies
- Peer
- Consensus
- Orderer

Architecture :





Implementation :

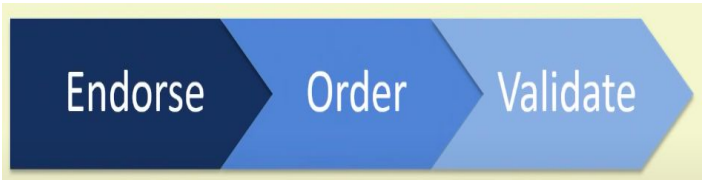
- HLF Client SDK provides the Fabric - ca - client, Fabric - common, and Fabric - network APIs to interact with the blockchain

Algorithms used by HLF:

- TLS 1.2/ 1.3 (RSA TLS)
- SHA256 for hashing
- pBFT consensus algorithm

Transaction Flow :

- Propose Transaction
- Execute Proposed Transaction
- Proposal Response
- Order Transaction
- Deliver Transaction
- Validate Transaction
- Notify Transaction



Transaction Flow :

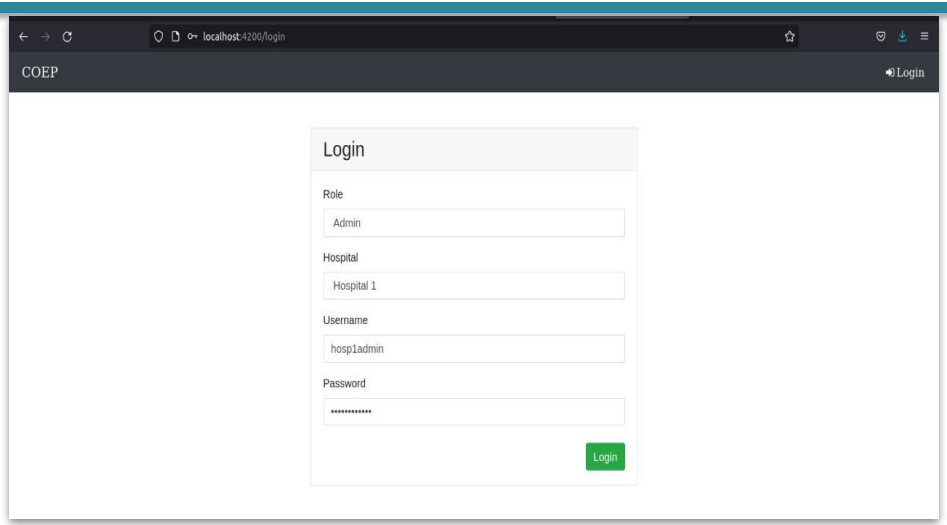
- Prerequisites

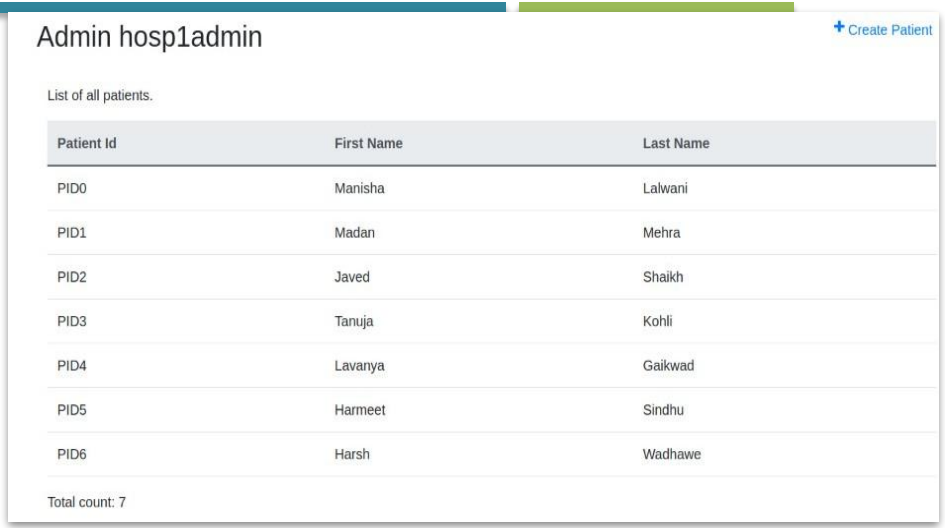
Install docker, node, npm, golang, curl tools. Download the fabric basic framework generating platform-specific binaries and Docker images.

- Start network

./network.sh up createChannel: Shows all docker containers needed for 2 hospitals and creates ’hospitalChannel’ on which both hospitals are connected.
./network.sh deployCC: Packages smart contract code and initial data of 6 patients is created in a ledger.

Application :



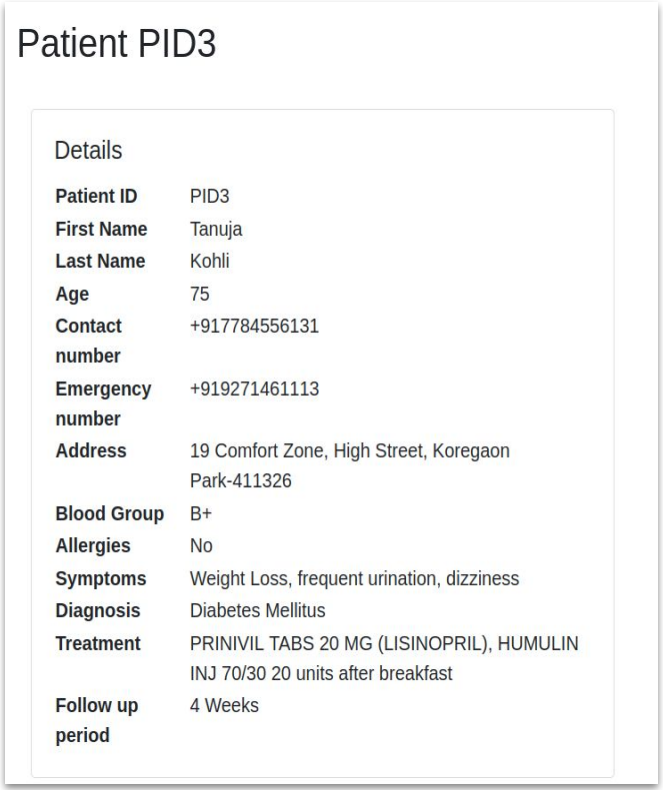


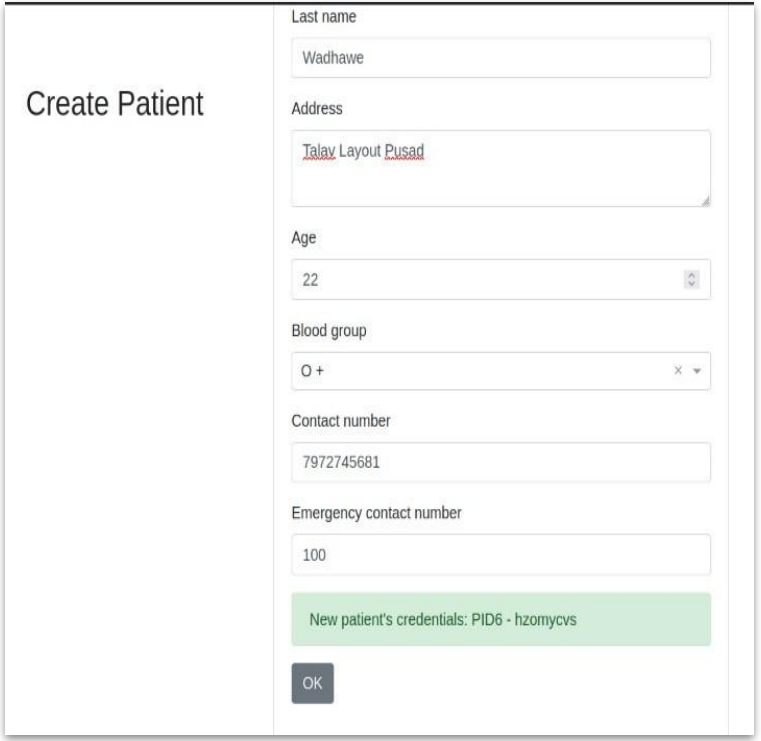
History of a patient.

Date	Last changed by	First Name	Last Name	Age	Blood Group	Address	Contact number	Emergency number	Allergies	Diagnosis	Symptoms	Treatment	Followup duration
Wed Feb 23 2022	initLedger	Tanuja	Kohli	75	B+	19 Comfort Zone, High Street, Koregaon Park-411326	+917784556131	+919271461113	No	Diabetes Mellitus	Weight Loss, frequent urination, dizziness	PRINIVIL TABS 20 MG (LISINOPRIL), HUMULIN INJ 70/30 20 units after breakfast	4 Weeks

Total count: 1

Application :





Comparison :

Traditional Database Systems

Susceptible to attacks like Denial of Service (DOS) and can lead to single point of failure.

If the private certificates of a user are disclosed or stolen, a malicious user can perform arbitrary Read and Write queries to the database. According to the established policy, the security of the system may be compromised.

Hyperledger Fabric

HLF is invulnerable to common **attack vectors** and avoids possibility of single point failure by storing data in decentralized manner with the same level of performance.

In our case, this scenario is unrealistic since no entity is completely authorized or has control over the ledger (not even the administrators).

Comparison :

Traditional Database Systems

Susceptible to attacks like Denial of Service (DOS) and can lead to single point of failure.

If the private certificates of a blockchain user are disclosed or stolen, a malicious user can perform arbitrary Read and Write queries to the blockchain ledger. According to the established policy, the security of the system may be compromised.

Hyperledger Fabric

HLF is invulnerable to common **attack vectors** and avoids possibility of single point failure by storing data in decentralized manner with the same level of performance.

In our case, this scenario is unrealistic since no entity is completely authorized or has control over the ledger (not even the administrators).

Results :

Why our solution is better:

- Access records faster during emergencies.
- Ethereum-based systems are limited by security guidelines requiring the preservation of participant information and access to datasets.
- In M2M (Machine-to-machine), dependence on others restricts flexibility.
- Processing power and time taken by encryption algorithms in IoT-based blockchains vary based on computational abilities.
- To enhance security, medical history is managed through the transaction history, which can reduce healthcare issues when implemented on a large scale.

Results :

Issues in HLF:

- getHistoryForKey - Private Data Collection.
- Create a user defined role instead of client.
- Access user attributes using client.

Challenges in developing the application:

- Implementing security mechanism
- Re-encryption - Node Js lacks a decent re-encryption library
- Tracking of public key of created user through fabric SDK
- Scaling of peers

Future Scope :

- Improvements to make this a production grade application.
- Use **Apaches Kafka**, an open-source distributed event streaming platform to manage multiple ordering nodes to handle transaction requests and approvals as the system scales.
- Store wallet in noSQL database and replicate to multiple nodes to avoid data loss.
- Integrate email functionality for temporary passwords & forgot password mechanism.
- Applying UI/UX strategies to enhance the user experience.
- Deploy application using **Kubernetes**, the best orchestration tool to manage containers. As the network grows, more hospitals with their peers and channels exist in the network.

Conclusion :

- HLF is a promising blockchain framework that comes with policies, smart contracts and provision of secure identities.
- Enable the EHR scenario interoperable among multiple hospital organizations.
- Promising framework for private & closed blockchain scenarios to manage data.
- Provide reliable and secure solution in managing medical field records.

References :

[1] Ahmed, M., Reno, S., Akter, N., & Haque, F. (2020, December). Securing medical forensic system using hyperledger based private blockchain. In 2020 23rd International Conference on Computer and Information Technology (ICCIT) (pp. 1-6). IEEE.

[2] Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M., & Schulte, S. (2020, November). ETH relay: A cost-efficient relay for ethereum based blockchains. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 204-213). IEEE.

[3] Alshalali, T., M'Bale, K., & Josyula, D. (2018, December). Security and privacy of electronic health records sharing using hyperledger fabric. In 2018 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 760-763). IEEE.

[4] Vardhini, B., Dass, S. N., Sahana, R., & Chinnaiyan, R. (2021, January). A Blockchain based Electronic Medical Health Records Framework using Smart Contracts. In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE.

[5] Abeywardena, K. Y., Attanayaka, B., Periyasamy, K., Gunarathna, S., Prabhathi, U., & Kudagoda, S. (2020, December). Blockchain based Patients' detail management System. In 2020 2nd International Conference on Advancements in Computing (ICAC) (Vol. 1, pp. 458-463). IEEE.

[6] " Hyperledger Fabric, " https://hyperledger-fabric.readthedocs.io/en/ release-2.2/ledger/ledger.html

[7] Fabric, H. (2021). The Ordering Service. Docs, Release-2.2,[Online]. Available: https://hyperledger-fabric. readthedocs. io/en/release2.2/orderer/ordering service. Html

[8] Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M. H., & Kerrache, C. A. (2021). The case of hyperledger fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1), 100012.

[9] Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. Sensors, 20(22), 6587.

References :

[10] Li, D., Wong, W. E., & Guo, J. (2020, January). A survey on blockchain for enterprise using hyperledger fabric and composer. In 2019 6th International Conference on Dependable Systems and Their Applications (DSA) (pp. 71-80). IEEE.

[11] Metnitz, P. G. H., & Lenz, K. (1995). Patient data management systems in intensive care—the situation in Europe. Intensive care medicine, 21(9), 703-715.

[12] J. Sousa, A. Bessani, and M. Vukolic, “A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform,” in Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, 2018, no. Section 4, pp. 51–58

[13] FILIPPO BOIANI,”Blockchain Based Electronic Health Record Management For Mass Crisis Scenarios”,STOCKHOLM, SWEDEN 2018.

[14] Castro, M.,& Liskov, B. (1999, February). Practical byzantine fault tolerance. In OsDI (Vol. 99, No. 1999, pp. 173-186).

[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” J. Gen. Philos. Sci., vol. 39, no. 1, pp. 53–67, 2008.

[16] Kotla, R., & Dahlin, M. (2004, June). High throughput Byzantine fault tolerance. In International Conference on Dependable Systems and Networks, 2004 (pp. 575-584). IEEE.

THANK YOU

Any Questions?