FitVault: Fitness data management with permissioned Blockchain Technology

MSc Research Project
Cloud Computing

Rohith Nair
Student ID: 231194898

School of Computing
National College of Ireland

Supervisor: Shreays Setlur Arun

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Rohith Nair……………………………………………………………………………………………

Student ID: 23119489………………………………………………………………………………………………..……

Programme: Msc. Cloud Computing…………………………… **Year:** 2023-24……….

Module: Research Project………………………………………………………………….………

Supervisor: Shreays Setlur Arun

Submission Due Date: 12th August, 2024…………………………………………………………………………

Project Title: FitVault: Fitness data management with permissioned Blockchain Technology

Word Count: 5375…………………………… **Page Count** 20…………………………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rohith Nair…………………………………………………………………………………

Date: 05th August 2024………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

FitVault: Fitness data management with permissioned Blockchain Technology

Rohith Nair
23119489
Github link - https://github.com/rohithn737/fianl_proj.git

Abstract

The integration of technology and healthcare has become has increased due to high speed internet and widespread use of smart devices. the study involves the application of Hyperledger Fabric, a permissioned blockchain technology which is enabled in a FitVault ecosystem which enhances the security and fitness of data. This approach will ensure a secure environment for data which is generated through healthcare system and fitness and wellness centers. IoT - Internet of Things and wearables has led to increase in the amount of personal and sensitive information. Traditional data management systems, cloud computing and edge computing, face challenges of latency issue and vulnerabilities over data transfer over unsecured networks.

Keywords: Hyperledger Fabric, Fitness Data Management, Blockchain Technology, Privacy, Healthcare, Fitness, Smart Devices, Encryption

1 Introduction

The fusion of healthcare and technology has led to attention among technologists and researchers. This is largely due to high-speed internet and wide use of smart devices in our daily life. The ecosystem has been improved by edge Computing, Cloud Computing and Data analytics which helps in preventing the PII (personally identifiable information) data. The main issues with these technologies is of latency, security issues during data transfer over unsecured channels. Fitness data along with permissioned blockchain technology, Hyperledger fabric can secure and individuals information in various ways.

Hyperledger Fabric is a permissioned blockchain technology that uses various techniques like encryption, digital signatures and smart contracts to prevent tampering of user's data while ensuring transparency and authenticity. The consensus is developed with the help of a consensus mechanism which allows transparency and authenticity of fitness data stored on the immutable block as part of blockchain network. Hyperledger Fabric is an open-source permissible blockchain platform that helps in the development of DApps (Decentralized Applications) for various industrial purposes like finance, healthcare, research where data security is the topmost priority.

Hyperledger Fabric offers a promising solution for data protection generated from fitness devices, institutions and healthcare system. The study aims to explore the poteintail of Hyperledger Fabric and how blockchain network helps in data accountability and privacy.

The introduction of 5G, along with enhanced security gives the user with the control of how their data flow through a system thus creating a robust platform for fitness data management.

1.1 Research Motivation

The popular usage of fitness devices and application s has resulted to growth of fitness data which is highly personal and sensitive. This surge in data production has led to creation of robust mechanisms to ensure data privacy and security of the users. Cloud computing, Edge Computing faces a serious concern of security and latency challenges when data is transferred over unsecured network channels. These challenges highlight the importance of more secure and fitness data management solution.

This led to address of more advanced blockchain technology, Hyperledger Fabric. Hyperledger Fabric is a permissioned blockchain technology which is known for its high security, flexibility and ability to handle complex data management tasks. It is decentralized and permissioned approach to data management which ensures safe and secure transfer of user data without compromising transparency and accountability.

Furthermore, this research seeks to demonstrate the potential of Hyperledger Fabric in revolutionizing fitness data management by addressing the following key points -

a) **Data Privacy and Security :** Hyperledger Fabric helps in protecting sensitive fitness data by giving permission to only authorized users over the channel .
b) **Transparency and Accountability :**transparency and accountability mechanisms in Hyperledger Fabric can be utilized for securing fitness data generated through various organizations.
c) **User Control and Consent:** Through Hyperledger Fabric empowers users with control over their personal data, which includes the ability to grant and revoke access.

1.2 Research Question

Can Hyperledger Fabric enhance security, privacy, scalability and regulatory compliance in FitVault's fitness data management ?

1.3 Report Structure

SECTIONS	**Introduction**
SECTION 2	Related work and Literature review
SECTION 3	Research Methodology
SECTION 4	Design Specifications
SECTION 5	Implementation of the proposed solution
SECTION 6	Evaluation
SECTION 7	Conclusion and Future Work

2 Related Work

The advancement in healthcare through digital technologies has made it necessary to ensure data security, privacy and interoperability. The literature review provides findings on application of blockchain technology, Hyperledger Fabric, to address challenges in the management of electronic health records. (EHRs)

2.1 Review of Technology in Health

The shift to Patient-Driven Healthcare

Farahani et al. (2018) looked into the transition from clinic-centric to patient-driven healthcare-systems, highlighting importance of technologies that has any anomaly detection and provides us with a early warning. The major challenges faced during this shift are data security, privacy, system scalability and method standardization. The patent-driven model could help us in providing more effective healthcare services but require immediate robust mechanisms to counter the challenges faced during the shift.

Drawish et al. (2019) investigated on integration of IoT and cloud computing for healthcare data management. The found out the need for robust data management system which would be better be scalable, storage system and a durable solution. The lack of these mechanism can lead to inconsistencies in implementing IoT and cloud solutions in healthcare systems leading to reduced efficiency and reliability of healthcare delivery.

Ahmadi et al.(2019) further categorized the Tech-Health ecosystems into multiple sub-domains such as Hospitals, Patient management systems, E-Health and Mobile health. They pointed out about the lack of standardized designs and interoperability as significant issues.

2.2 Review of Data Security

Enhancing Data integrity and Authentication

Sicari et al.(2015) has proposed architecture for Tech-Health systems, which focuses on privacy, access control and authentication however the authors did not emphasize much on architectural design. This can lead to difficulties in implementing and standardizing security protocols across various platforms and devices within the healthcare systems.

Sfar et al.(2018) vulnerabilities in IoT system security thus proposing a system/framework focused on access control, data privacy and authentication. However eternal threats found in the communication channels can lead to failure of the propose architecture.

Aksu et al.(2017) proposed a risk assessment methodology which quantifies various risk levels based on various predefined metrics on internal and eternal threats. They did not adequately address secure storage of PII. This becomes crucial for the data kept at rest in the storage systems, which is target by the attack which can lead to risk of loss of sensitive information.

2.3 Review of Data Privacy

Alshalali et al. (2018) further discusses the advantage of using Hyperledger Fabric for managing EHRs. They mentioned about the advantage of using blockchain technology which provides access levels, allowing users with complete control of their data on how it is communicated through different channels. The decentralized approach help in preventing sensitive data, thus creating data integrity and preventing unauthorized manipulations. It also emphasizes on cryptographic keys and digital certificates in securing the share of the data in blockchain network across various channels.

Benhammouda et al. (2018) investigates about secure multipart computation(MPC) with Hyperledger Fabric to handle private data transactions securely. The private data is encrypted through MPC. This paper strengthens combining blockchain and cryptographic techniques thereby enhancing the overall security framework of EHRs.

Udden et al.(2021) proposed a Hyperledger Fabric system to improve the interoperability, scalability and availability of EHR systems. it involves creation of ledger network with channels enabled for private communication between the organization enrolled as part of the channel. This lead to creating a immutable environment for storing and sharing EHRs. This ensures data segregation, privacy and collaboration among different organization involved in the channel.

Use Cases and Applications

Kumar and Dakshayini(2020) presents a practical application of Hyperledger Fabric of how securely patient data can be share among healthcare organizations. Trust and security can be achieved with the help of features of blockchain technology such as distributed technology such as distributed channels, chaincodes, encryption. This application shows the potential of blockchain technology in the healthcare domain which provides decentralized, immutable transactions ensuring transparency and accountability.

Antwi et al. (2021) investigate the feasibility of using Hyperledger Fabric and testing various scenarios on how different scenarios for testing security can help in confidentiality, flexibility, privacy and scalability in healthcare applications. This tells us about the versatility of Hyperledger Fabric in meeting diverse security and operational requirements int he fitness and healthcare sector.

Wang and Quin (2021) addresses the need for interoperability through proposing a permissioned blockchain technology, Hyperledger Fabric. This is developed with chaincodes with hierarchical access control to strengthen privacy protection in data sharing. This helps in improving the existing data storing systems to enhance data security and interoperability. This approach highlights potential of blockchain which can be integrated with existing systems making it a suitable solutions for fitness and healthcare providers.

Uddin et al. (2021) propose a Hyperledger Fabric mechanism architecture for different EHR system to improve interoperability, scalability and availability. This involved where organizations are enrolled over secured channels on a ledger network where consensus mechanism is achieved through chanicodes. This architecture enables a private channels for the healthcare stakeholders. This ensures the segregation of data ensuring privacy while collaborating with different organizations.

Several studies highlight the privacy preserving mechanisms in the healthcare data management systems. The integration of MPC(multiparty computation) and use of encryption of private data through Hyperledger Fabric led to further advancement and research in this area. This ensures secure data transfer with authorized parties over a ledger network. 13-Benhamouda et al.(2018) demonstrated how MPC can be used to handle private data transactions securely without comprising the integrity and functionality of the system.

Based on the most papers evaluated above does not address the issues related to data access, privacy management and access control for sensitive user health and fitness data at its core architecture in the Tech-Health ecosystem. Our proposed architecture shall make use of core principles of Blockchain technology, Hyperledger Fabric technology, Distributed channels, and immutable block technology to improve upon the security and privacy aspects of the Tech-Health ecosystem.

3 Research Methodology

In this section we shall discuss the concepts of the building blocks that from the basis of our proposed system, FitVault system.

The research methodology follows research work is based on concept Agile Software Development process. Agile methodology reduces obstacles that may affect the research process. It promotes quick learning from continuous feedback mechanisms. It helped in identifying gaps in the process and continuously improve the process without affecting the objective.

3.1 Overview of Research Methodology

The research methodology help us in understanding the evaluation of blockchain technology and its application on maintaining the fitness data management with the help of permissioned blockchain technology, Hyperledger Technology. Testing data has been presented in the form of scenarios, we first need to establish the majority requirements required of the fitness data management. The goal of the research activity is establish that the goal of this research activity is to identify key requirements and math against the results of test sets when implemented on Hyperledger Fabric network. A full production ready application will not be ready in this project but will have scope for that too.

3.2 Research Phases

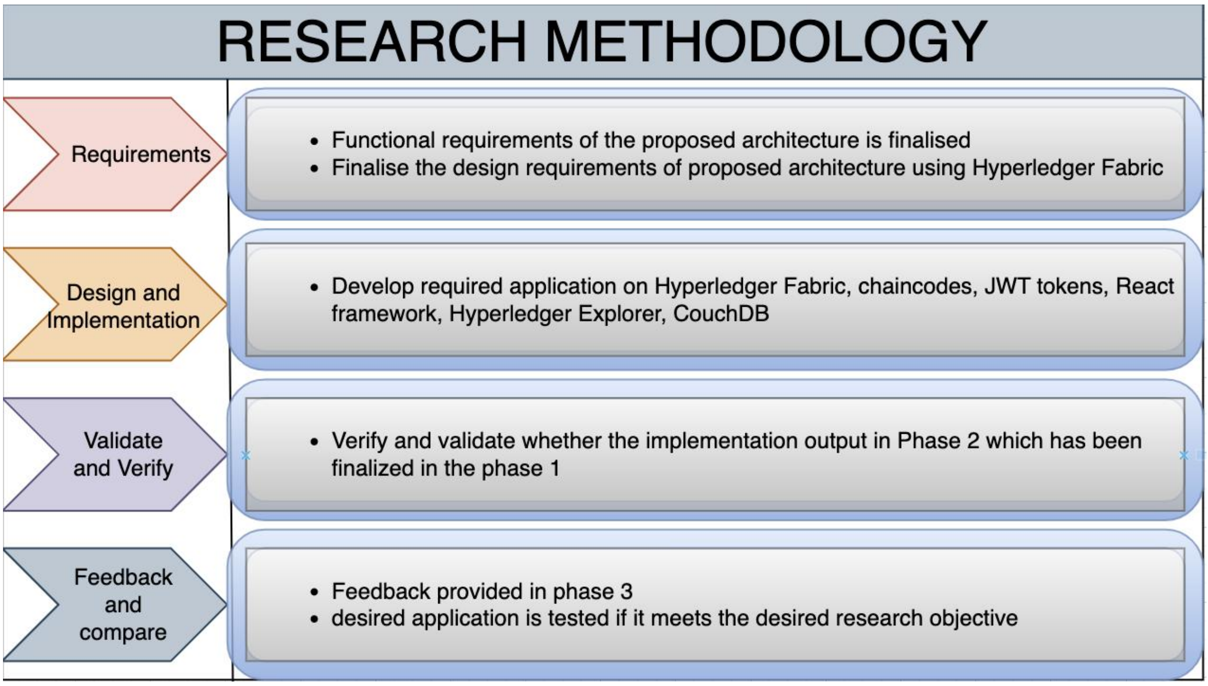
The research methodology consists of the following phases -

1) Requirements :

a) Identify and finalize the functional requirements of the proposed architecture
b) Define the design requirements for implementing the proposed architecture using Hyperledger Fabric and related technologies

2) Design:

a) Develop detailed design specifications for the proposed architecture.
b) Create design prototypes to visualize the proposed solution in the Hyperledger Fabric network



- Functional requirements of the proposed architecture is finalised
- Finalise the design requirements of proposed architecture using Hyperledger Fabric

- Develop required application on Hyperledger Fabric, chaincodes, JWT tokens, React framework, Hyperledger Explorer, CouchDB

- Verify and validate whether the implementation output in Phase 2 which has been finalized in the phase 1

- Feedback provided in phase 3
- desired application is tested if it meets the desired research objective

Figure 1: Overview of Research Methodology

3) Develop and Implement:

a) Implement the designed applications on Hyperledger Fabric using couchDB, Chaincode, JSON Web Tokens, React Framework, Hyperledger Explorer, MongoDB and postman.
b) Develop the necessary software components and integrate them into the blockchain environment

4) Validate and Verify:

a) Verify and validate whether the implementation meets the requirements defined in the initial phase
b) Perform the validations to ensure the architecture performs as expected

5) Feedback and Compare:

a) Collect feedback based on the validation and verifiaction phase
b) Compare the results against the desired research objectives
c) Iterate and refine the methodology based on the feedback to improve the solution

3.3 Ethical Considerations

To adhere to data ethics requirements, the presented research did involve amny PII - personally Identifiable Information or any other kind sensitive information which can affect any user/person. Dummy data has been used as part of this research papers for the purpose of demonstration of how data flow happens through network channel between different organizations which are part of the channel.

4 Design Specification

Through the proposed design our aim is to have a system with high privacy, security and transparency for managing fitness data generated through devices, fitness centers and healthcare systems. The architecture is designed in such a way for efficient and safe handling of sensitive data.

4.1 Hyperledger Fabric - An Introduction

Hyperledger Fabric, a permissioned blockchain technology has the ability to provide decentralized, secure and transparent data management system. Hyperldeger Fabric, is a used to meet the privacy, security and consensus of th data flow through the channels in the system .

Key components of Hyperledger Fabric:

1) **Peer:** Peers are the fundamental building blocks of Hyperledger Fabric network. They host ledgers and smart contracts and have two types of peers -
    a) **Endorsing peers :** These peers help in endorsing transactions based on chaincodes. They are responsible for validating transactions between the peers which will be committed in the ledger.
    b) **Committing peers :** Peers commit the valid transactions to the ledger. Every peer in the network act as committing peer.
2) **Chaincodes (Smart contracts) -** Business logic of the blockchain network. Rules for the transaction are defined in the chaincodes. chaincodes are written in JavaScript, Go, Java.
3) **Consensus Mechanism:** Rules on how blockchain transactions are executed and agreed upon by participating nodes in the blockchain network.
4) **Transaction:** Information transfer between two blockchain address or the peers in the channels through chaincodes.
5) **Block:** A storage unit for performing batch of transactions, distributed to all participating peers involved in the channel and blockchain network.
6) **Chain :** A sequence of immutable blocks
7) **Membership Service Provider(MSP):** Manages identities and roles of network participants
8) **Channel**: Pre-approved participants are only allowed on a blockchain network are able to execute the transactions
9) **Orderer**: A central hub for communication for creation of the blocks and are maintained over a consistent ledger state in the network.
10) **Communication Channel(CA) :** Communication channels helps in establishing a secure communication between nodes/peers.
11) **Certifying Authority(CA):** Issues public and private keys and signs certificates thus verifying the participants involved in the network.

12) **Ledger:** The database are replicated across all the peers for maintaining the latest transactions data in each peer within the channel.
13) **Web Application:** Front-end application created using React and JavaScript as programming language for the users to interact with blockchain network.
14) **Entities:** Participants such as fitness trainers, doctors, users, administrators are the participants in the blockchain network known as entities.

4.2 Benefits in the Fitness Data Management

Hyperledger Fabric offers significant advantages for managing fitness data:

1) **Data confidentiality:** Permissioned access ensures only authorized participants can access sensitive data in the channel
2) **Data Integrity:** Immutable records are maintained through cryptographic hashing method
3) **Data Availability:** High fault-tolerance due to decentralized storage
4) **Access Control:** Smart contracts help in maintaining consensus mechanisms.

4.3 Architecture

The architecture for proposed fitness data management system includes several key components for a secure and effecient data handling as illustrated in Fig. 2

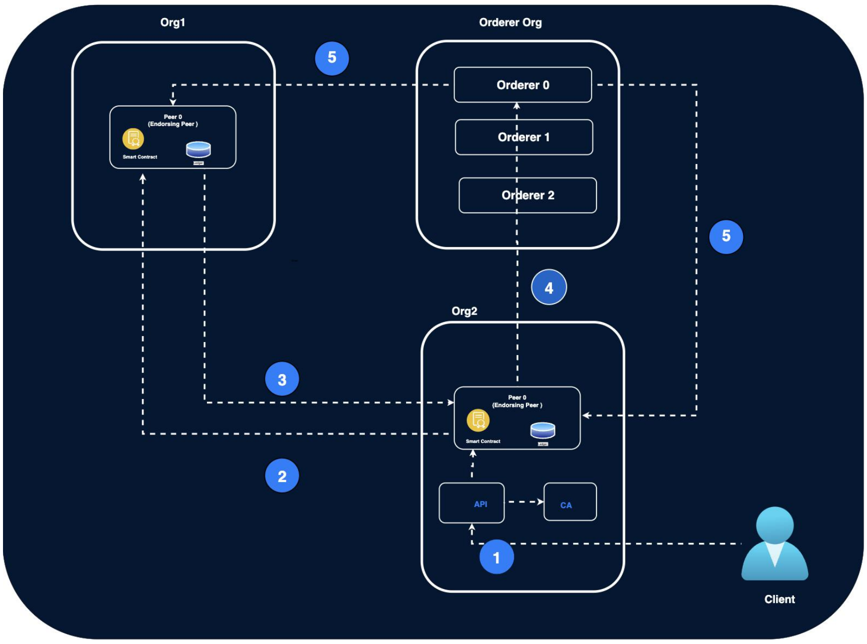


Figure 2 Proposed Architecture

4.4 Privacy and Security Considerations

Privacy and security of fitness data is of topmost priority. Proposed architecture uses the following below given mechanism -

1) **Private Data Collection** : Sensitive data is stored securely on the nodes using hashing and encryption techniques and only authorized entities are allowed to access this information
2) **Smart Contracts**: Business logic of the blockchain network. Rules for transactions are defined in the chaincodes. Chaincodes are written in JavaScript, Go, Java.
3) **Access Control** - Access control is managed through the MSP and its validated through the chaincode.
4) **Data Encryption** - Ensures data privacy and integrity through hashing algorithm

5 Implementation

The implementation phase of this research focuses on developing and integrating the necessary components for the proposed fitness data management system using Hyperledger Fabric. This section outlines the steps and technologies used to realize the proposed architecture.

5.1 Setting Up Hyperledger Fabric

The Hyperledger Fabric network is set up and configured to support the fitness data management system. This involves creating a test network and configuring the nescessary components.

Steps:

1) **Install Prerequisites:** Install Docker, Docker Compose, Postman, Hyperledger Explorer, Node.js, and Hyperledger Fabric binaries and samples.
2) **Network Setup:** Basic network is setup in hyperledger network using Hyperledger Fabric binaries and samples. Modify configuration files to include specific organizations and peers(3 peers) required for the fitness data management system.
3) **Channel creation:** Channel is created for 2 peer organizations and 1 orderer organizations for fitness data management. Each organizations has to join the channel to participate in the network after approval from Certificate Authority(CA).
4) **Generate Certificates:** Certificate Authority(CA) generates necessary certificates for identities (admin, peers, orderers) and manage the MSP.

5.2 Developing Chaincode

Business logic of the blockchain network, Hyperledger Fabric network. Rules for transaction are defined in the chaincodes. Chaincodes are written in JavaScript, Go, Java. Current implementation of chainocodes has been done on JavaScript(JS).

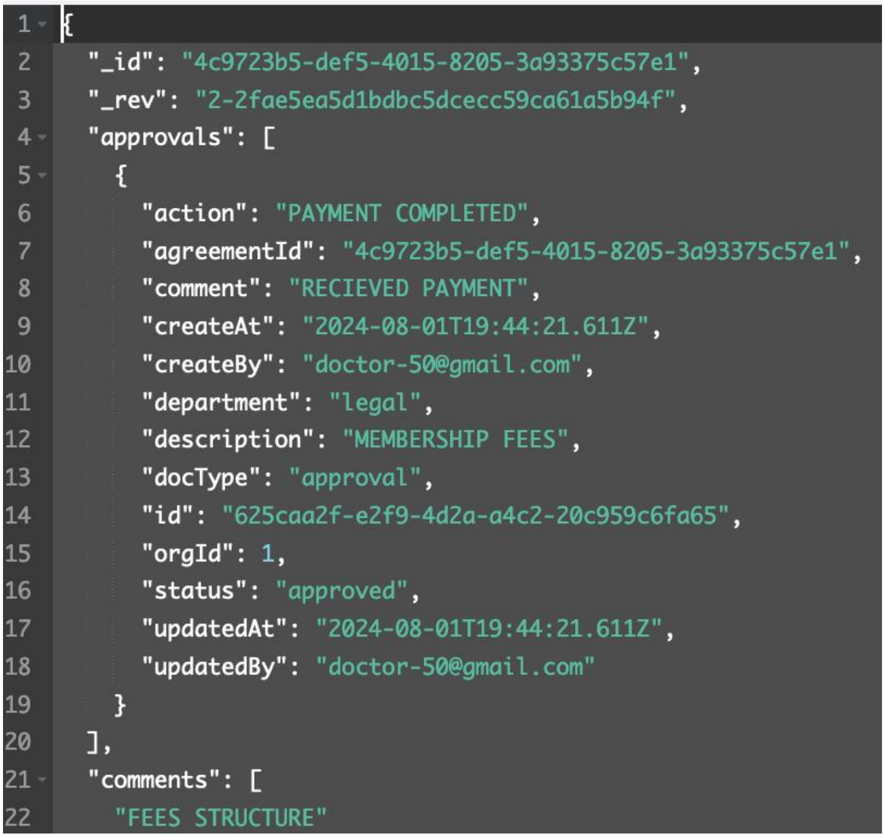
Steps:

1) **Define Business Logic:** A business logic is created for creating, updating and quering fitness records for different organizations which are part of Hyperledger Fabric network channel.
2) **Chaincode Implementation:** Implementation of the chaincode in the programming language - JavaScript. The chaincode includes function for creating fitness records,updating data, quering information.

3) **Package and Install chaincode :** Packaging of the chaincode and installing it on the endorsing peers of each organization in the channel.
4) **Instantiate Chaincode**: Instantiate the chaincode on the channel, making it available for execution which could fulfill the organization's request.

Implemented Function in chaincode:

1) **Create Record:** Creates a new fitness record for a user or enroll a new user which can be part of any organization in the channel
2) **Update Record:** Updates existing fitness data/task for a user. Update the nescessary state of the chaincodes based on request by the organizations.
3) **Query Record:** Query data for a user/approval state based on specified criteria



```
{
  "_id": "4c9723b5-def5-4015-8205-3a93375c57e1",
  "_rev": "2-2fae5ea5d1bdbc5dcecc59ca61a5b94f",
  "approvals": [
    {
      "action": "PAYMENT COMPLETED",
      "agreementId": "4c9723b5-def5-4015-8205-3a93375c57e1",
      "comment": "RECIEVED PAYMENT",
      "createAt": "2024-08-01T19:44:21.611Z",
      "createBy": "doctor-50@gmail.com",
      "department": "legal",
      "description": "MEMBERSHIP FEES",
      "docType": "approval",
      "id": "625caa2f-e2f9-4d2a-a4c2-20c959c6fa65",
      "orgId": 1,
      "status": "approved",
      "updatedAt": "2024-08-01T19:44:21.611Z",
      "updatedBy": "doctor-50@gmail.com"
    }
  ],
  "comments": [
    "FEES STRUCTURE"
```

Figure 3 Sample Data Record - Chaincode Implementation - CouchDB

5.3 Setting up distributed ledger

The distributed ledger stores all the transactions stores al the information securely as immutable transaction. For ledger data , Hyperledger Fabric has been utilized , which provides a user friendly interface for monitoring and interacting with Hyperledger Fabric network. Key advantages of using Hyperledger Fabric networks are -

1) Enhanced visibility and Transparency
    a) Real-time monitoring
    b) Detailed Metrics
2) User-friendly Interface
    a) Intuitive Dashboard
    b) Easy Navigation

3) Simplifies Network Management

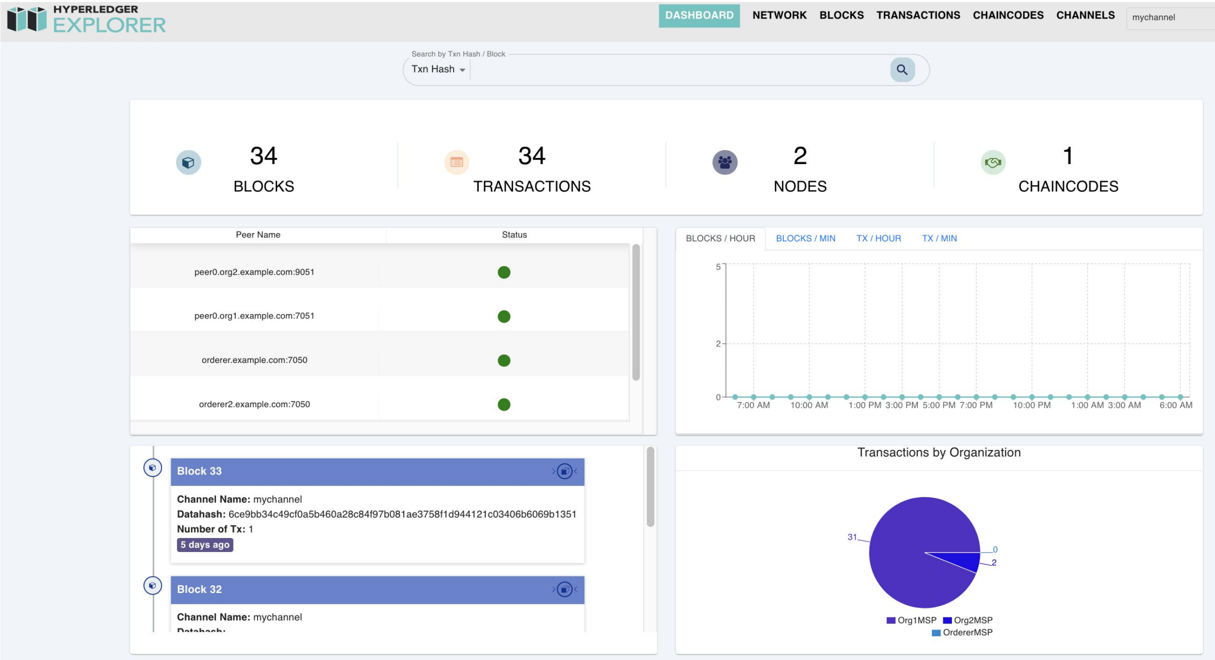
    a) Network configuration
    b) Channel Management

4) Improved Debugging and Troubleshooting

    a) Transaction Details
    b) Block Inspection

5) Enhanced Security Compliance

    a) Access Control



Peer Name	Status
peer0.org2.example.com:9051	●
peer0.org1.example.com:7051	●
orderer.example.com:7050	●
orderer2.example.com:7050	●

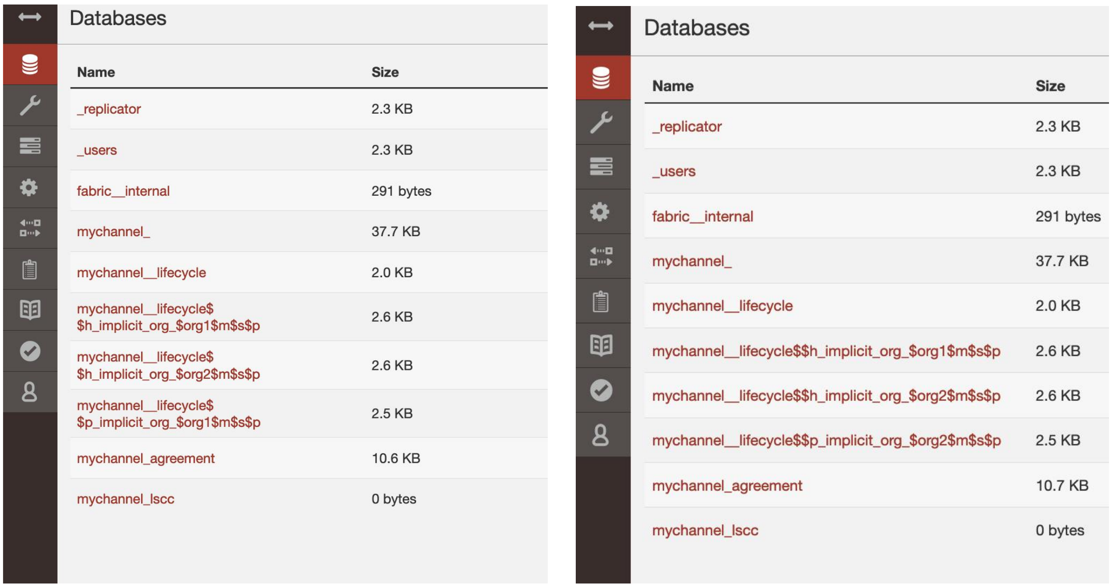
Block 33

Channel Name: mychannel
Datahash: 6ce9bb34c49cf0a5b460a28c84f97b081ae3758f1d944121c03406b6069b1351
Number of Tx: 1
5 days ago

Block 32

Channel Name: mychannel

Figure 4 Hyperledger Explorer blockchain network interface



Databases

Name	Size
_replicator	2.3 KB
_users	2.3 KB
fabric__internal	291 bytes
mychannel_	37.7 KB
mychannel__lifecycle	2.0 KB
mychannel__lifecycle$$h_implicit_org_$org1$msp	2.6 KB
mychannel__lifecycle$$h_implicit_org_$org2$msp	2.6 KB
mychannel__lifecycle$$p_implicit_org_$org1$msp	2.5 KB
mychannel_agreement	10.6 KB
mychannel_lscc	0 bytes

Databases

Name	Size
_replicator	2.3 KB
_users	2.3 KB
fabric__internal	291 bytes
mychannel_	37.7 KB
mychannel__lifecycle	2.0 KB
mychannel__lifecycle$$h_implicit_org_$org1$msp	2.6 KB
mychannel__lifecycle$$h_implicit_org_$org2$msp	2.6 KB
mychannel__lifecycle$$p_implicit_org_$org2$msp	2.5 KB
mychannel_agreement	10.7 KB
mychannel_lscc	0 bytes

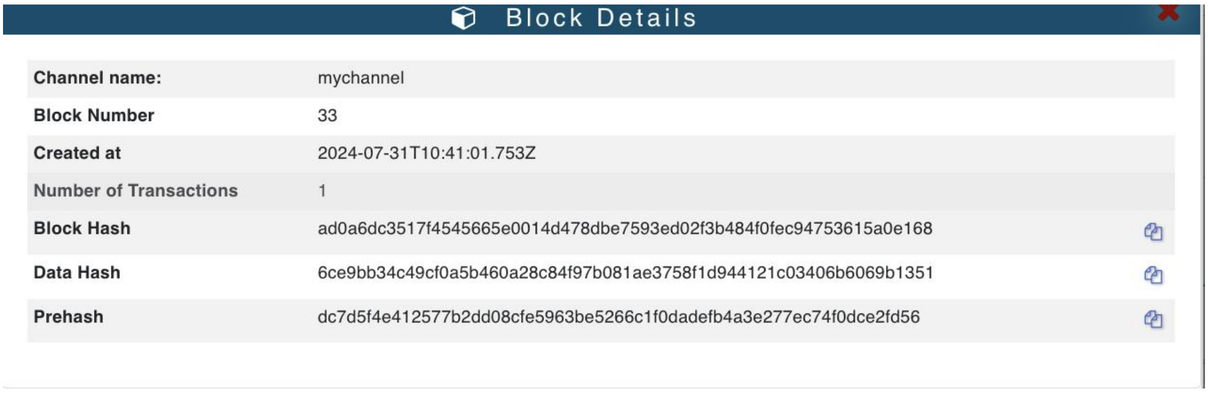
Figure 5 CouchDB configuration for org1 and org2

Steps for Distributed Ledger : -

a) **Configure Database:** CouchDB will be used as current state database for storing fitness data in JSON format. Through postman API calls, data can be fetched from couchDB for the requested organization part of the channel - mychannel

b) **Initialize Ledger:** Initializing the ledger by deploying the chaincode and creating initial fitness records for testing purpose.

c) **Perform Transactions -** Transactions are executed through chaincode to create, update and query fitness records, ensuring ledger is updated consistently across all the peers. Once transaction has been verified, orderer peer will send signed transaction if the parent peer of the respective organization to place transaction on the ledger as a new block



Channel name:	mychannel
Block Number	33
Created at	2024-07-31T10:41:01.753Z
Number of Transactions	1
Block Hash	ad0a6dc3517f4545665e0014d478dbe7593ed02f3b484f0fec94753615a0e168
Data Hash	6ce9bb34c49cf0a5b460a28c84f97b081ae3758f1d944121c03406b6069b1351
Prehash	dc7d5f4e412577b2dd08cfe5963be5266c1f0dadefb4a3e277ec74f0dce2fd56

Figure 6 Block Transaction details

5.4 Hyperledger Fabric SDK

The Hyperledger Fabric provides a set of tools for the developers to interact with the Hyperledger Fabric network. SDK helps in creation of chaincodes, which helps in perform transactions and querying in the network.

Key features of Hyperledger Fabric SDK -

1) Chaincode deployment and management of chaincode:

- **a) Chaincode deployment: T**hrough the help of Postman, APIs are used to install and instantiate chaincodes on peers which allows business logic/chaincodes to be defined between peers participating in the network
- **b) Invoke chaincode:** invoking APIs to perform certain functions, which leads to execution of transactions ultimately updating the ledger
- **c) Query Chaincode:** APIs can be used to fetch the transactions stored in the ledger without modifying the current state of the transaction.

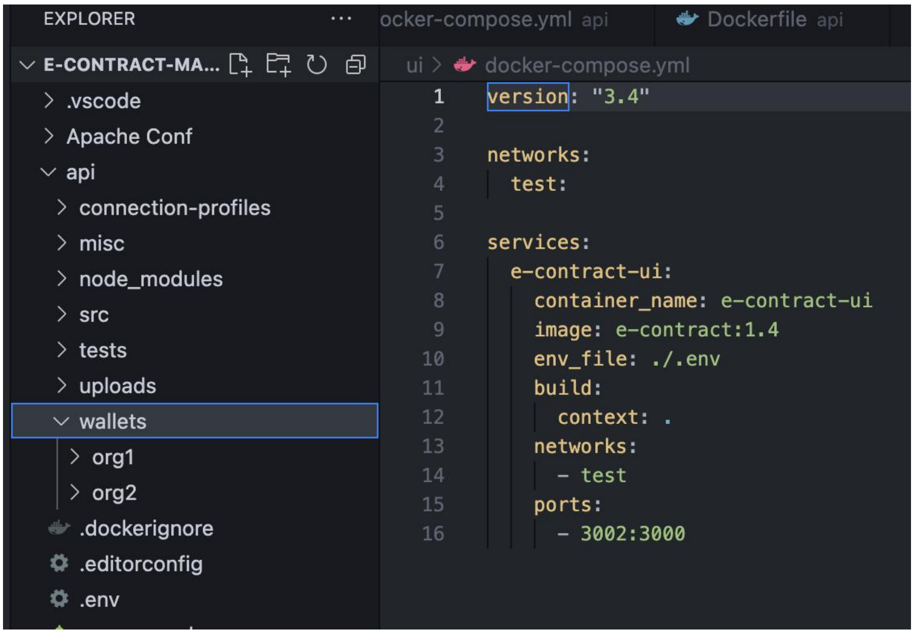
2) Network Creation

- a) **Connection Profiles**: Connection profiles are used in the SDK for network configuration including the details of peers, orderers, and channels.
- b) **Gateway:** Efficient communication in the blockchain network is maintained through SDKs gateway

c) **Event Handling**: SDK provides mechanism for handling blockchain events when a block commits and transactions is succeeded

3) **Identity Management:**

a) **Wallet**: wallet is used for managing user identities, which includes digital signature and private keys of the peers involved in the channel
b) **MSP Integration**: Network participants enrolling in the blockchain network are authorized by MSP



```yaml
version: "3.4"

networks:
  test:

services:
  e-contract-ui:
    container_name: e-contract-ui
    image: e-contract:1.4
    env_file: ./.env
    build:
      context: .
    networks:
      - test
    ports:
      - 3002:3000
```

Figure 7: Wallets for org1 and org2

Hyperledger Fabric SDK is used for below purposes:

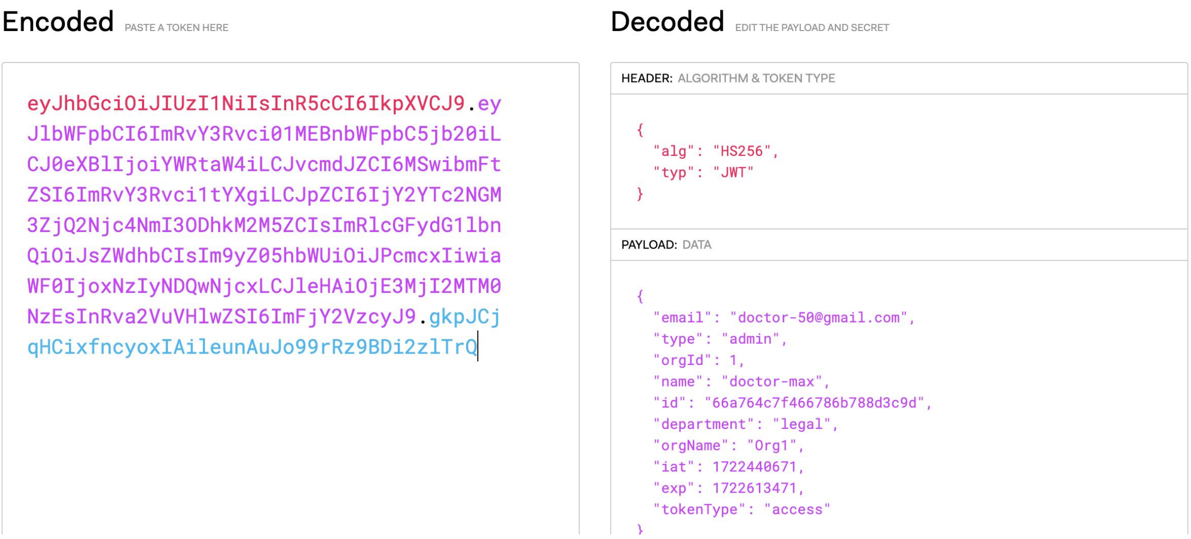
1) **Initializing network connections:** Connections profiles which are part of Hyperledger Fabric Samples are used for setting up connection to hyperledger Fabric network
2) **User Authentication :** Authenticate users using their digital signatures stored in the wallet
3) **Invoke transaction:** Transactions can be invoked by authorized parties(e.g, administrators, fitness trainers, doctors, users) to create, update and query fitness data records.
4) **Handle Events:** SDK provides mechanism for handling blockchain events when a block commits and transactions is succeeded.

5.5 JSON Web Tokens(JWT)

JSON Web tokens (JWT) are a compact, URL-safe means of representing claims between two parties. They are widely used for authentication and authorization purposes in web applications.

Key features of JSON web tokens:

a) Compact and URL-safe
b) Self-contained
c) Signed


Encoded PASTE A TOKEN HERE
Decoded EDIT THE PAYLOAD AND SECRET
HEADER: ALGORITHM & TOKEN TYPE
PAYLOAD: DATA

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JlbWFpbCI6ImRvY3Rvci01MEBnbWFpbC5jb20iL
CJ0eXBlIjoiYWRtaW4iLCJvcmdJZCI6MSwibmFt
ZSI6ImRvY3Rvci1tYXgiLCJpZCI6IjY2YTc2NGM
3ZjQ2Njc4NmI3ODhkM2M5ZCIsImRlcGFydG1lbn
QiOiJsZWdhbCIsIm9yZ05hbWUiOiJPcmcxIiwia
WF0IjoxNzIyNDQwNjcxLCJleHAiOjE3MjI2MTM0
NzEsInRva2VuVHlwZSI6ImFjY2VzcyJ9.gkpJCj
qHCixfncyoxIAileunAuJo99rRz9BDi2zlTrQ
```

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

```
{
  "email": "doctor-50@gmail.com",
  "type": "admin",
  "orgId": 1,
  "name": "doctor-max",
  "id": "66a764c7f466786b788d3c9d",
  "department": "legal",
  "orgName": "Org1",
  "iat": 1722440671,
  "exp": 1722613471,
  "tokenType": "access"
}
```

Figure 8 JWT token of an dummy user part of “mychannel” blockchain network

JWT usage in Hyperledger Fabric network -

a) Authentication of users
b) Authorize access
c) Session Management

JWT Usage in Fitness Data Management System -

a) User Login
b) Authenticated Requests
c) Chaincode Invocation
d) Event handling

5.6 Wallets in Hyperledger Fabric SDK

In the Hyperledger Fabric, wallets are used to manage identities (certificates and private keys) for users and applications that interact with the blockchain network. the wallet makes sure only authorized users can perform actions on blockchain such as invoking chaincodes or quering the ledger.

Key Features of Wallets:

a) Identity Management
b) Secure Storage
c) Integration with MSP

Types of Wallet:

a) File system wallet
b) Hardware Security module wallet (HSM)
c) Cloud-based wallet

Wallet are used in Hyperledger Fabric Network:

Wallets are used to manage the identities of diffeent participants (e.g, administrators, fitness trainers, users) and ensure secure interactions with the blockchain network.

a) **Enrollment of Identities**
b) **Admin Enrollment:** These credentials are stored in the wallet. Administrators are enrolled by Certificate Authority by creation of public and private keys
c) **User Enrollment:** Users are enrolled by the admin. Users can be doctors, fitness trainers and users whose credentials are stored in the wallet
d) **User Authentication:** User's Identity is retrieved from the wallet when user logs into the web application. The identity of the user includes a signed certificate from CA and a private key through which the user is authenticated into the network

Chaincode Invocation:

a) Transaction Proposal
b) Endorsement
c) Submission

Querying the Ledger:

a) Identity Retrieval
b) Query Execution

5.7 Deploying Web application

A web application using JavaScript and React, is developed to provide an inetrface for users (administration, fitness trainers, and users) to interact with the the blockchain network.

Steps:

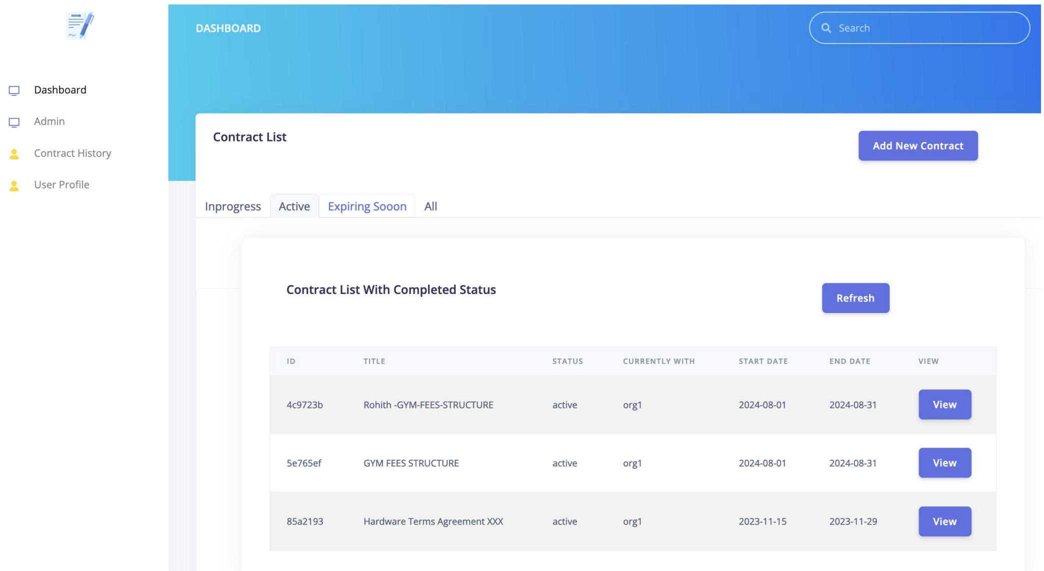
1) **Choose Framework:** Use React Framework to build a user-friendly and responsive web application
2) **Create User Interfaces:** Develop different views for administrators, fitness trainers, and users. Each view provides specific functionalities based on the user's role.
3) **Integrate with blockchain:** Use the Hyperledger Fabric SDK for node.js to inetract with the blockchain network. The web application communicates with the blockchain using the PI hit from postman to execute transactions and query data.
4) **Testing and Validation:** testing and validation are crucial to ensure the system meets defined requirements and performs as expected

Deployment

Once the system has been thoroughly tested and validated, it can be deployed in production environment. A full production ready application will not be ready in this project but will have scope for that too.

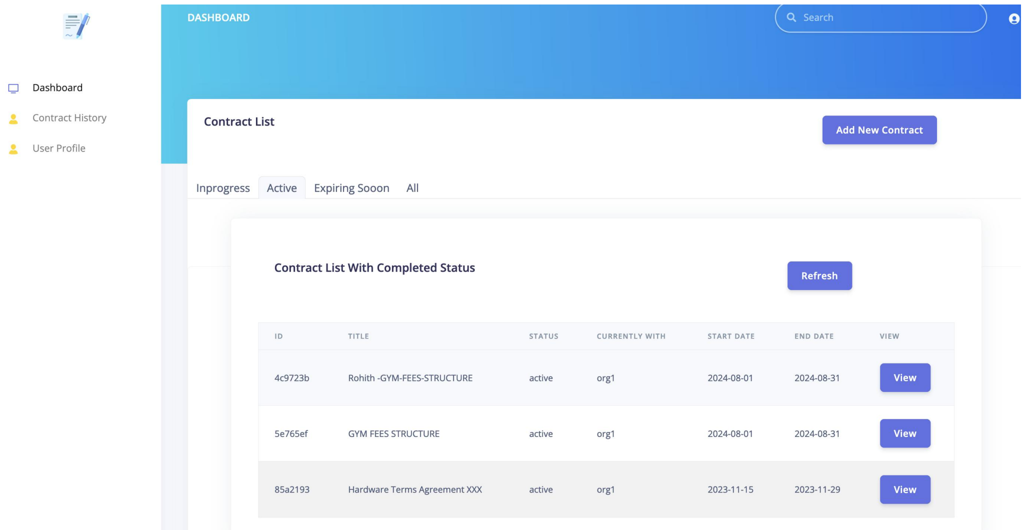
Steps -

1) **Setting up Network:** configure a Hyperledger Fabric network with high availabilityand fault tolerance
2) **Deploy Chaincode:** Deploying the finalized chaincodes on to the network
3) **Launch Web Application:** Deploy the web application on a secure server, ensuring it is accessible to users.
4) **Monitor and Maintain:** Continuously monitor the system for performance and security issue, applying updates and improvements as necessary.



ID	TITLE	STATUS	CURRENTLY WITH	START DATE	END DATE	VIEW
4c9723b	Rohith -GYM-FEES-STRUCTURE	active	org1	2024-08-01	2024-08-31	View
5e765ef	GYM FEES STRUCTURE	active	org1	2024-08-01	2024-08-31	View
85a2193	Hardware Terms Agreement XXX	active	org1	2023-11-15	2023-11-29	View

Figure 9: Admin console

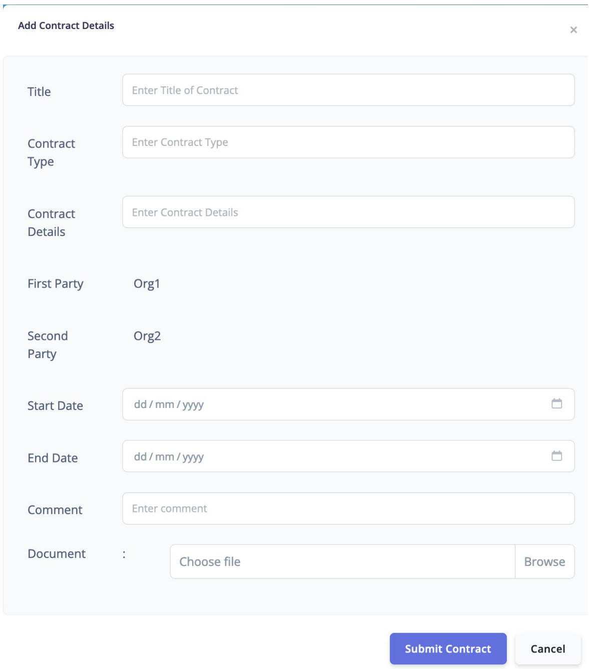


ID	TITLE	STATUS	CURRENTLY WITH	START DATE	END DATE	VIEW
4c9723b	Rohith -GYM-FEES-STRUCTURE	active	org1	2024-08-01	2024-08-31	View
5e765ef	GYM FEES STRUCTURE	active	org1	2024-08-01	2024-08-31	View
85a2193	Hardware Terms Agreement XXX	active	org1	2023-11-15	2023-11-29	View

Figure 10: User console

6 Evaluation

In this section, we evaluate the proposed FitVault architecture by examining various scenarios related to storage, data privacy, and data security. It has been divided inot 3 sections - storage, data privacy and data security to ensure it meets the requirements an objectives of the research project.



Add Contract Details

Title: Enter Title of Contract
Contract Type: Enter Contract Type
Contract Details: Enter Contract Details
First Party: Org1
Second Party: Org2
Start Date: dd / mm / yyyy
End Date: dd / mm / yyyy
Comment: Enter comment
Document : Choose file

Figure 11: Smart Contract creation

Data Storage

This category assesses the system's capability to handle storage-related tasks, such as creating and modifying fitness records. The following scenarios were tested:

It will also deal with how efficiently the designed system is in accordance with the research objective to handle storage-related tasks which include creation, modification of records. The below scenarios were tested -

SCENARIO	RESULT
An authorized user can create a trasanction (fitness record)	Successful
An authorized user can update/modify a record	Successful
An authorized user can create a smart contracts with doctors and fitness trainers	Successful

Data Privacy

Data privacy for nay system is most critical. The following scenarios were tested to ensure data privacy for the proposed architecture:

SCENARIO	RESULT
User Interface for the homepage depends on the user (Admin, Fitness Trainers, doctors, users)	Successful
A user requires special permissions to be invoked to view other user's data	Successful
A user can grant/revoke access from UI interface when allowed by the admin user	Successful

Data Security

Data security is another crucial aspect addressed in the FitVault architecture. The following scenarios were tested to ensure enhanced security levels in the system

SCENARIO	RESULT
Use of private data collections to avoid tampering of data	Successful
MSP ID verificatio before granting access to a user within the channel and network	Successful
Data Integrity is maintained through hashing algorithms and JWT tokens	Successful
Metadata as well as agreement used in the chaincodes are securely stored in the cloud S3 buckets and in the blocks (encrypted form)	Successful

7 Conclusion and Future Work

The integration of Hyperledger Fabric in the FitVault ecosystem has shown significant advancements in management of fitness data. Through this research critical issues like data privacy, security and transparency has been addressed with permissioned blockchain technology. Through this system fitness data is stored securely maintaining its integrity and authenticity. The key findings of this research include:

a) **Enhanced Data Privacy and Security:** Encryption algorithms, digital signatures and smart contracts has shown significant advancements on how fitness data can be securely managed on a Hyperledger network. Implementation of Private Data collections strengthens data privacy by only authorized users having access to personal identifiable information (PII).
b) **Transparency and Accountability:** Decentralization nature of blockchain technology provides an immutable and transparent ledger of all transactions, enhancing
c) **User control and consent:** The system empowers users by providing control of their own data where users can revoke/grant access to their data giving full control on how their data has been utilized
d) **Scalability and Flexibility:** To meet the market requirements, Hyperledger Fabric's architecture is able to scale and customize according to the need.

In conclusion , the FitVault system powered by Hyperledger Fabric offers a promising solution for secure and private management of fitness data. The systems design ensures that data privacy, security, and user control are priortized, addressing key concerns in the fitness and healthcare industry.

7.1 Future Work

As with any emerging technology there are opportunities for further improvement and exploration. Further work in this area could focus on the following aspects -

a) Enhancement in scalability: We can sale the architecture to include more organizations and users, this involves integrating more advanced consensus and storage mechanisms to handle huge data loads effectively.
b) Integration with Advanced Technologies: Further Hyperledger Fabric can be integrated with IoT and AI technologies. This could be enhance real-time data processing which can solve more complex security, privacy concerns for fitness data
c) Regulatory Compliance with network: Ensuring compliance with evolving data protection regulations, such as GDPR, will be crucial. Future work could focus on developing automated compliance checks and integrating them into the blockchain network.
d) User Experience Improvements: Enhancing user interface and experience to make it more intuitive and user-friendly for a wider adoption. This can be enabled for mobile applications and improving control access mechanisms.

By focusing on these areas, future research can be build on the foundation laid by this research to enhance security, privacy, and usability of fitness dara management by users.

References

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N. and Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, pp.659–676. doi:https://doi.org/10.1016/j.future.2017.04.036.

Darwish, A., Hassanien, A.E., Elhoseny, M., Sangaiah, A.K. and Muhammad, K. (2017). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), pp.4151–4166. doi:https://doi.org/10.1007/s12652-017-0659-1.

Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J. and Yang, X. (2018). A Survey on the Edge Computing for the Internet of Things. IEEE Access, 6, pp.6900–6919. doi:https://doi.org/10.1109/access.2017.2778504.

Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M. and Alizadeh, M. (2018). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society, [online] 18. doi:https://doi.org/10.1007/s10209-018-0618-4.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, [online] 76, pp.146–164. doi:https://doi.org/10.1016/j.comnet.2014.11.008.

Riahi Sfar, A., Natalizio, E., Challal, Y. and Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, [online] 4(2), pp.118–137. doi:https://doi.org/10.1016/j.dcan.2017.04.003.

Tantawy, A., Abdelwahed, S., Erradi, A. and Shaban, K. (2020). Model-Based Risk Assessment for Cyber Physical Systems Security. Computers & Security, 96, p.101864. doi:https://doi.org/10.1016/j.cose.2020.101864.

Naveen Kumar S and M. Dakshayini (2020). Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology. doi:https://doi.org/10.23919/icombi48604.2020.9203442.

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Habib ur Rehman, M. and Kerrache, C.A. (2021). The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications. Blockchain: Research and Applications, 2(1), p.100012. doi:https://doi.org/10.1016/j.bcra.2021.100012.

Wang, Q. and Qin, S. (2021). A Hyperledger Fabric-Based System Framework for Healthcare Data Management. Applied Sciences, 11(24), p.11693. doi:https://doi.org/10.3390/app112411693.

Uddin, M., S. Memon, M., Memon, I., Ali, I., Memon, J., Abdelhaq, M. and Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. Computers, Materials & Continua, 68(2), pp.2377–2397. doi:https://doi.org/10.32604/cmc.2021.015354.

Alshalali, T., M'Bale, K. and Josyula, D. (2018). Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric. 2018 International Conference on Computational Science and Computational Intelligence (CSCI). doi:https://doi.org/10.1109/csci46756.2018.00152.\