Software Design Document for project Decentralization of medical records using BlockChain Technologies.

Linette Joseph
Neha Susan Manoj
Muhammed Hashir PM
Mohammed Nazeem C

Supervised by: Prof. DILEESH E D

December 13, 2022

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to give a detailed description of our project , DeMed : Demonstration of a secure decentralized application as an alternative to the current centralized medical records management system. This software design document describes the architecture and system design of DeMed. It is intended for both the designers, developers as well as end-users of the system.

1.2 Scope

The "DeMed" will be a platform used for Demonstration of a secure decentralized application as an alternative to the current centralized medical records management system. The patient's information should be uploaded to our application by the user. These specifics are added to the Polygon Blockchain, and a block's transaction hash is obtained. The specific information the user submitted may be retrieved using this hash. The system will be designed to:

- To get around the centralization issue.
- To store health records over decentralized network so that they cannot be tampered with.
- To keep track of the data associated with patients' Ethereum public addresses, guaranteeing the patient anonymity.
- Blockchain is anonymous, so it successfully maintains trust between node-to-node.

1.3 Overview

Section 2 of this document gives an system overview about the product.It describes a general description of the functionality, context and design of your project. Section 3 gives more specific information about the functionalities specified in section 2 that contains the system architecture . Section 4 is data design which has the data description and dictionary . In Section 5 ,component design we take a closer look at what each component does in a more sys- tematic way. Section 6 , Human Interface design gives an overall overviw of user interface .Section 7 contains the requirement matrix that provide a cross reference that traces components and data structures to the requirements in your SRS document. Section 8 contains references.

1.4 Reference Material

1. IEEE SDD Standard -SDD-ieee-1016-2009.pdf in local folder

1.5 Definitions and Acronyms

Term	Definition
Hash	An Identifier which helps to find a particular transaction in the Blockchain network
User	A person who wants to upload details or retrieve details from the application

2 System Overview

The function of our system is secure and transparent storage and transmission of medical information between patients and various health organizations. The system includes the followings functionalities:

• Patient-defined access to medical information: Users may choose who they wish to share their medical data with, rather than having to make it available to all healthcare organisations.
• Transfer of medical data: When using the decentralised storage technique, it is possible to request medical data instantly and securely.

The key functions of the product are:
In case a patient visits of a medical institution :
• A patient gives a temporary access to his/her data.
• A smart contract will temporarily unlock the patient's medical record for making changes, while the medical institution uses its identifier to access the required data.
• Patient's medical records are updated.
• The patient can see the changes of the record.
Other participants of the system:
• The patient provides access to the records of his record for other participants of the system.
• A smart contract defines the mechanism of interaction with unlocked patient data.
• The patient can at any time get an access to his medical record through a single portal of public services.

3 System Architecture

3.1 Architectural Design

Figure 1 abstracts the overall architecture of the project. The user interacts with the Blockchain system using a software interface. The patient and the doctor has separate interfaces in the application.The doctor can add the record of the patient and view the medical history if the access is granted.

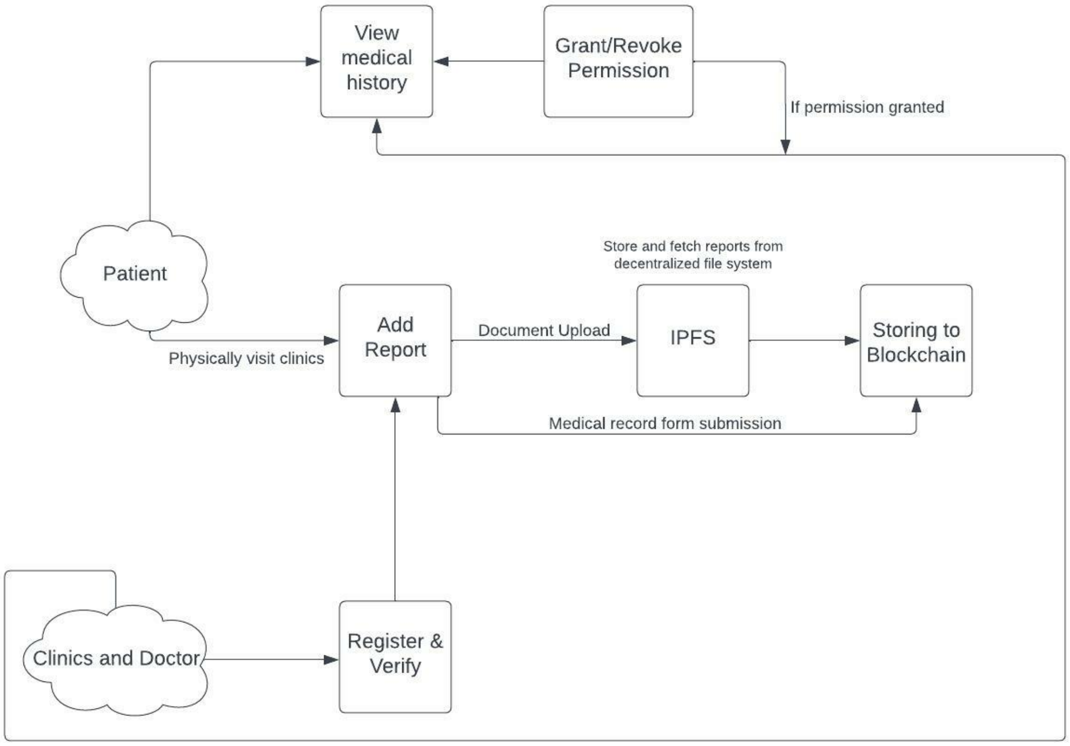


Figure 1: Architectural Design

3.2 Decomposition Description

The System is divided into 4 modules based on the functionality of the system. A concise summary of the module and its functionality is provide below. The Modules are :-

- Authentication - This Module mainly deals with the user Authentication. The user would sign in with a metamask wallet and depending on the type of user they will redirected to the respective interfaces.

- Medical History - If the type of user is patient -they can view their medical history and grant/revoke access to individual record.

- Add a medical record - If the type of user is a doctor ,they can view the medical history of the patient if the access is granted and they can add a new medical record against the patient id.

- Interacting with blockchain - Adding and retrieving data from the blockchain is facilitated through smart contracts written in solidity and whenever the user needs to interact with the blockchain ,particular instances of the smartcontracts is invoked.

3.3 Use Case Design

A use case diagram is a dynamic or behavior diagram in UML. Use case diagrams model the functionality of a system using actors and use cases. Use cases are a set of actions, services, and functions that the system needs to perform

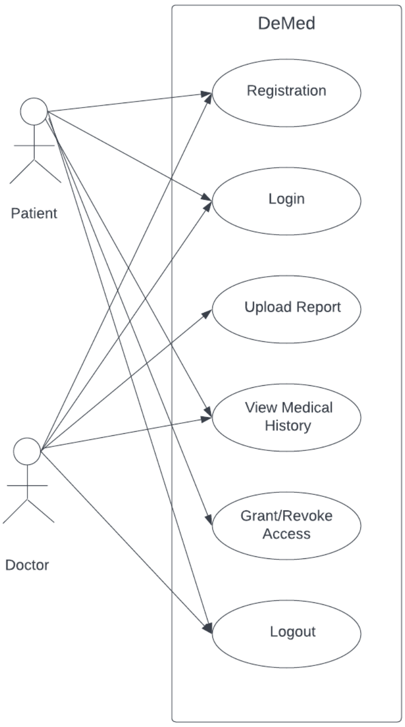


Figure 2: Use case diagram

3.4 Design Rationale

We have selected the architecture given in the above figure because the 4 module which we have have described in section 3.2 can be independently developed and integrated. These modules can be integrated after the unit testing and hence there is least chance for errors. The other architecture under considerations was to use a centralized server which in turn interacts with the blockchain.But the problem with these architectures are that , it would make the entire system slow and if the server goes down the entire system would fail.

4 Data Design

4.1 Data Description

The data domain of DeMed is patients' medical records. If there are any documents (for example x-ray) they are uploaded to Interplanetary File System (IPFS) and its corresponding hash value is obtained.
This IPFS hash value can be stored along with the other medical record data directly

into the Blockchain in the form of string data type which is entered by the doctor on completing a form.
The format of the medical record data is defined as a struct data structure. The user holds a mapping from his/her wallet address to a list of struct

4.2 Data Flow

- Patient : The user will login to the system using metamask wallet address .The user data and medical data associated with the wallet address is obtained from the blockchain and is displayed in the user interface.The patient can grant/revoke access to these medical records.
- Doctor : The user will login to the system using metamask wallet address .The type of user associated with the wallet address is obtained from the blockchain and the medical record that is required is displayed if the access is granted.
- System : The system acts as an interface between the user and the blockchain
- Blockchain: All the required information stored in the blockchain and can be required whenever it is required,

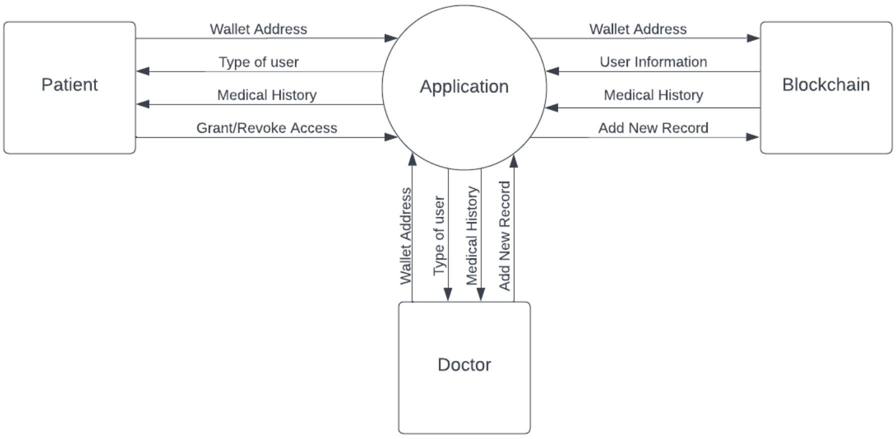


Figure 3: Dataflow diagram

5 Human Interface Design

5.1 Overview of User Interface

A user interface is essentially a tool that, depending on access controls, enables a person to access medical records quickly. Each user has a place where they can log in and register. Access control is offered in accordance with their role. Health providers can update the system with new data. Although data updates are possible, there will still be references to earlier data. A patient can see medical records history. A doctor can edit and update medical records pertaining to various patients.
The interface would have the following functionalities:

5.1.1 User Authentication using wallet

There is a button labelled "Connect with wallet." Metamask notification will appear upon clicking. The application allows for anonymous user authentication.

5.1.2 Uploading medical records to blockchain

The user fills a medical prescription template in the application and the data is uploaded to the Blockchain.

5.1.3 Viewing the history of all medical records of a particular patient

The user can choose to examine all of their health records and grant and revoke particular access to each one.

5.2 Screen Images

Display screenshots showing the interface from the users perspective. These can be hand drawn or you can use an automated drawing tool. Just make them as accurate as possible.

5.3 Screen Objects and Actions

A discussion of screen objects and actions associated with those objects.

5.3.1 Authentication Page:

- Continue Button : If the user is already authenticated with the metamask account, you can directly login to the appllication through the respective wallet address.

- Patient Button : If the user has not already signed in and wants to register as patient, then user can authenticate and create an account by connecting the wallet address using metamask.

- Health Organization Button : If the user has not already signed in and wants to register as Health Organization, then user can authenticate and create an account by connecting the wallet address of each doctors in the organisation using metamask and verifying by the Organization ID.

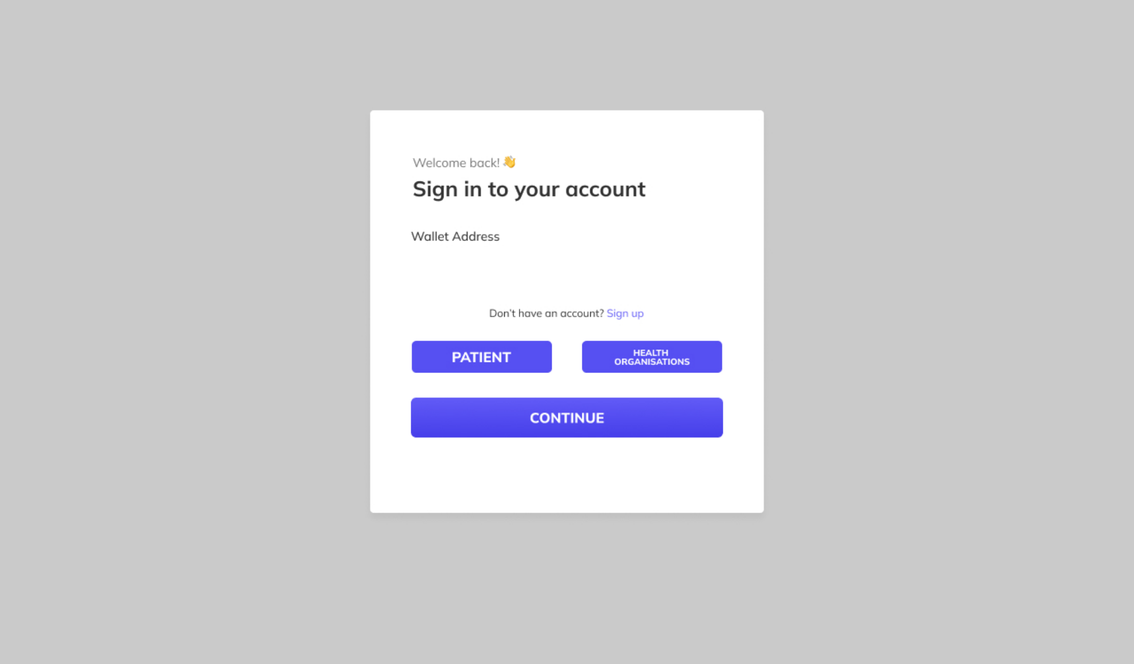


Figure 4: User Authentication using wallet.

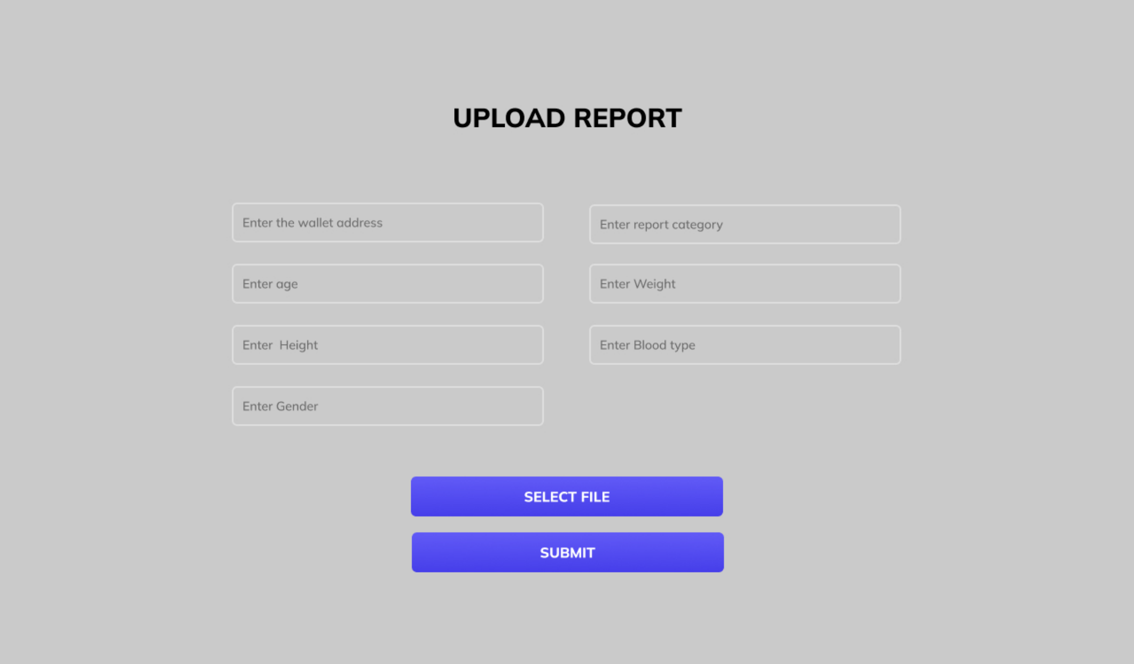
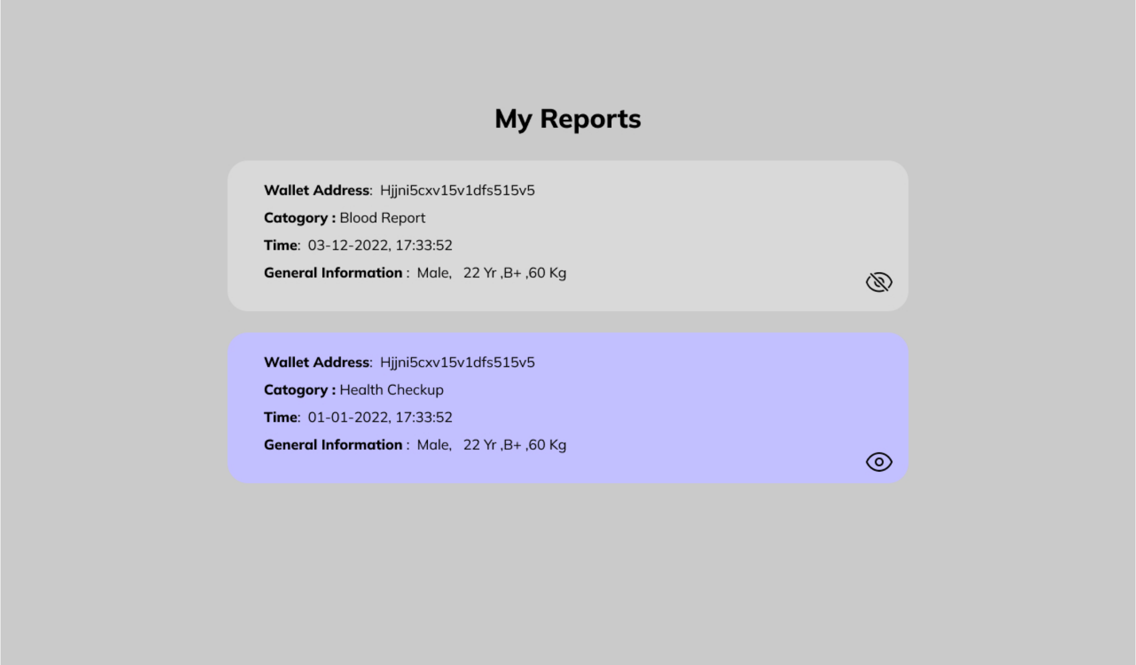


Figure 5: Uploading medical records to blockchain.



My Reports

Wallet Address: Hjjni5cxv15v1dfs515v5
Catogory : Blood Report
Time: 03-12-2022, 17:33:52
General Information : Male, 22 Yr ,B+ ,60 Kg

Wallet Address: Hjjni5cxv15v1dfs515v5
Catogory : Health Checkup
Time: 01-01-2022, 17:33:52
General Information : Male, 22 Yr ,B+ ,60 Kg

Figure 6: Viewing the history of all medical records of a particular patient.

5.3.2 Upload Reports Page:

- Required information must be entered
- Select File Button : This option is used to upload any relevent medical documents/records pertaining to the patient (X-rays , Test Reports)
- Submit Option :The entered information is stored in the blockchain (if it is a text) and documents are upoloaded to IPFS. The entered data cannot be changed.

5.3.3 Reports Page:

- Previous medical consultation history: Displays the relevent medical data from various consultation with timestamp.
- Patient can grant access to a organization or health providers to view his report history as per requirement.Either patient can grant access on all the reports or pick which reports to be shown.

6 References

[1] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30, 2016.

[2] Eman-Yasser Daraghmi, Yousef-Awwad Daraghmi, and Shyan-Ming Yuan. Medchain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access*, 7:164595–164613, 2019.

[3] Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, and Shaikh Akib Shahriyar. Doc-block: A blockchain based authentication system for digital documents. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pages 1262–1267, 2021.

[4] Meet Shah, Mohammedhasan Shaikh, Vishwajeet Mishra, and Grinal Tuscano. Decentralized cloud storage using blockchain. In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, pages 384–389, 2020.

[5] Ayesha Shahnaz, Usman Qamar, and Ayesha Khalid. Using blockchain for electronic health records. *IEEE Access*, 7:147782–147795, 2019.