PROVENANCE AWARE VERIFICATION AND AUDITING OF BLOCKCHAIN BASED EHR SYSTEM

A PROJECT REPORT

Submitted by

SHRRUTHI ND

(2023246034)

A report for the phase-I of the project
submitted to the Faculty of

INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment
for the award of the degree
of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600 025

DECEMBER 2024

ANNA UNIVERSITY

CHENNAI - 600 025

BONA FIDE CERTIFICATE

Certified that this project report titled PROVENANCE AWARE VERIFICATION AND AUDITING OF BLOCKCHAIN BASED EHR SYSTEM is the bona fide work of SHRRUTHI ND who carried out project work under my supervision. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion on this or any other candidate.

PLACE:	**DR. S. SWAMYNATHAN**
DATE:	**PROFESSOR**
	PROJECT GUIDE
	DEPARTMENT OF IST, CEG
	ANNA UNIVERSITY
	CHENNAI 600025

COUNTERSIGNED

DR. S. SWAMYNATHAN
HEAD OF THE DEPARTMENT
DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600025

ABSTRACT

Blockchain technology is the next revolution in the management of data because it has offered a decentralized, secure, and transparent system to provide solutions for applications where trust and integrity are very crucial. Healthcare is one sector that uses Electronic Health Records as an efficient tool for patient care challenges such as data breaches, unauthorized access, and lack of traceability deter the use of robust digital solutions. While blockchain-based EHR systems promise many advantages, most of them fail to address critical gaps such as fine-grained access control, comprehensive auditing, and provenance tracking.

To overcome these limitations the proposed system Provenance Aware Verification and Auditing in Blockchain-based EHR Systems has been introduced. The proposed utilizes blockchain's immutability and transparency to ensure secure and traceable EHR management. Patients will have control over access to their records, where selectively they will grant access to doctors for update consultation under transparent, smart contract-driven processes. The proposed system bridges the gaps existing with current solutions, providing integral data integrity, privacy, and trust among participants.

The outcome of the proposed system in phase I is to develop a patient centric system where patients and doctors can access the patient electronic health record only if access is provided by the patient. The outcomes in phase II are to develop a completely decentralized insurance claim based on the EHR and implementing it in private chain for interoperability.

ABSTRACT TAMIL

ACKNOWLEDGEMENT

It is my privilege to express my deepest sense of gratitude and sincere thanks to **Dr. S. SWAMYNATHAN,** Professor , Department of Information Science and Technology, College of Engineering, Guindy, Anna University, for his constant supervision, encouragement, and support in my project work. I greatly appreciate the constructive advice and motivation that was given to help me advance my project in the right direction.

I am grateful to **Dr. S. SWAMYNATHAN,** Professor and Head, Department of Information Science and Technology, College of Engineering Guindy, Anna University for providing us with the opportunity and necessary resources to do this project.

I would also wish to express my deepest sense of gratitude to the Members of the Project Review Committee: **Dr. S. SRIDHAR,** Professor, **Dr. G. GEETHA,** Associate Professor, **Dr. D. NARASHIMAN,** Teaching Fellow Department of Information Science and Technology,College of Engineering Guindy, Anna University, for their guidance and useful suggestions that were beneficial in helping me improve my project.

I also thank the faculty member and non teaching staff members of the Department of Information Science and Technology, Anna University, Chennai for their valuable support throughout the course of our project work.

SHRRUTHI ND
(2023246034)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 ELECTRONIC HEALTH RECORD (EHR)

An Electronic Health Record (EHR) is a comprehensive digital version of a patient’s medical history, designed to be accessible by authorized healthcare providers. It integrates a wide range of health data such as medical diagnoses, medications, lab results, allergies, treatment plans, and more [1] [2]. EHR systems are transformative in modern healthcare as they provide real-time access to critical patient data, helping healthcare providers make more informed decisions and improving patient care. These systems allow better care coordination, ensuring that all involved parties are updated about a patient’s treatment, reducing errors, and facilitating communication between healthcare providers [1] [3].

The introduction of EHRs has led to significant improvements in healthcare efficiency. By centralizing patient information in a digital format, healthcare providers can access data quickly and securely, eliminating the inefficiencies of paper-based records and minimizing the potential for human error [4] [5]. This centralization helps streamline various processes, including medical billing, insurance claims, and appointment scheduling, resulting in reduced administrative costs [6].

Moreover, patient empowerment has been greatly enhanced with the implementation of EHRs. Through patient portals, individuals can access their medical records, track their health conditions over time, and communicate directly with healthcare providers, promoting a sense of autonomy and involvement in their own healthcare journey [7] [8].

1.2 DISTRIBUTED STORAGE OF EHR

The distributed storage of Electronic Health Records (EHRs) is a critical aspect of modern healthcare systems, particularly when using blockchain and cloud technologies. Traditional centralized EHR systems often involve storing sensitive patient data on a central server, which can be vulnerable to cyberattacks or data breaches. Distributed storage, on the other hand, stores data across multiple, geographically dispersed servers, thereby mitigating the risks associated with single point of failure [6] [3].

Distributed storage systems are particularly effective in the context of blockchain, where data is stored in a decentralized manner across a network of nodes. This ensures that no single entity has complete control over the data, which enhances security and reduces the likelihood of unauthorized access [9] [5]. Additionally, the use of cryptographic techniques ensures that data is securely encrypted during storage and transfer, further protecting patient privacy.

In blockchain-based healthcare systems, patient data can be split into smaller encrypted fragments and stored across multiple nodes. Each fragment is then linked back to the patient's identity via a cryptographic hash. This ensures that even if one node is compromised, the data remains secure [1] [4]. Distributed storage systems also offer greater scalability and flexibility, enabling healthcare providers to store large volumes of data without overwhelming a single centralized server [10] [11].

1.3 SECURITY CONCERNS IN EHR STORAGE

Despite the numerous benefits of EHR systems, security remains a major concern in the storage of medical data. Healthcare data is highly sensitive, and any unauthorized access or modification can have serious consequences for patient privacy and safety [5] [12]. Traditional centralized storage systems are vulnerable to cyberattacks, such as hacking, ransomware, or data breaches, which could result in the theft or loss of sensitive medical information.

One of the main security concerns in EHR storage is ensuring data encryption, both at rest and during transmission. Encryption ensures that even if unauthorized individuals access the storage system, they will be unable to read or manipulate the data [13] [5]. In addition, access control mechanisms must be implemented to ensure that only authorized users, such as doctors, patients, or administrators, can access specific data [14] [15].

Another critical security challenge is data integrity, ensuring that the stored medical records are not tampered with or altered in unauthorized ways. Blockchain technology offers a promising solution to this problem, as its immutability guarantees that once data is recorded, it cannot be changed without detection [16] [4]. Additionally, regular auditing and verification of data integrity can help identify any discrepancies or unauthorized modifications in a timely manner [2] [8].

1.4 BLOCKCHAIN

Blockchain technology, originally introduced as the foundation for Bitcoin, has evolved into a versatile tool for various applications, including healthcare. A blockchain is a decentralized, distributed ledger that records data in a chain of blocks, where each block contains a set of transactions. These blocks are cryptographically linked, ensuring the integrity of the data. Once data is recorded in a block, it cannot be altered, creating a tamper-proof record [6] [14].

In healthcare, blockchain has the potential to revolutionize the way medical data is stored and shared. Blockchain ensures that healthcare data is immutable, transparent, and secure. Since blockchain is decentralized, there is no central authority controlling the data, which reduces the risks of data breaches and unauthorized access [5] [16]. Moreover, blockchain's consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensure that the network of nodes maintains consistency and data accuracy [17] [9].

1.4.1 Structure of Blockchain

- **Block:** A block is a data structure containing a set of transactions. Each block consists of:
  - **Header:** Includes metadata such as the block number, timestamp, previous block hash, and nonce.
  - **Transactions**: A list of validated transactions within the block.
  - **Merkle Root:** A hash summarizing all transactions in the block, derived using the Merkle tree.

- **Chain:** Blocks are linked sequentially, with each block referencing the hash of the previous one. This linkage ensures the integrity of the entire blockchain.

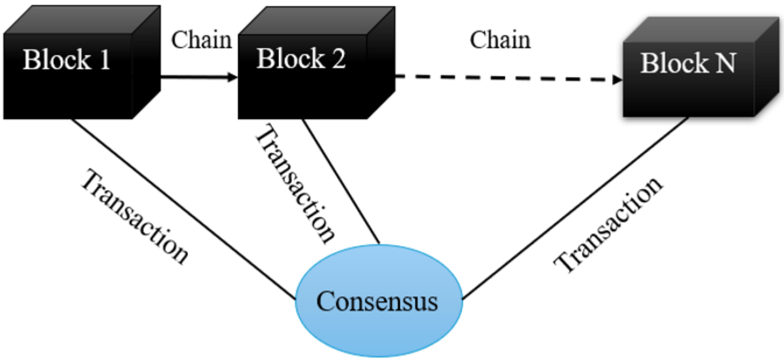


Figure 1.1: Structure of Blockchain

1.4.2 Consensus Mechanism

Consensus mechanisms ensure that all nodes in a blockchain network agree on the validity of transactions. Popular mechanisms include:

- **Proof of Work (PoW):** Nodes compete to solve complex mathematical puzzles, consuming computational power. Bitcoin uses PoW to secure its network.
- **Proof of Stake (PoS):** Validators are selected based on the amount of cryptocurrency they hold and are willing to "stake." PoS is more energy-efficient than PoW.
- **Delegated Proof of Stake (DPoS):** Stakeholders elect delegates to validate transactions and maintain the network.

- **Practical Byzantine Fault Tolerance (PBFT):** Nodes achieve consensus by communicating with each other, tolerating a limited number of malicious nodes.

1.4.3 Cryptographic Techniques

- **Hashing:** Ensures data integrity by producing unique fixed-size outputs for given inputs.
- **Digital Signatures:** Use private and public keys to authenticate transactions.
- **Encryption:** Secures sensitive information shared within the blockchain network.

1.4.4 Types of Blockchain

- **Public Blockchain :** Public blockchains are open to anyone who wants to participate. They are fully decentralized and often use PoW or PoS consensus mechanisms. Examples include Bitcoin and Ethereum. Public blockchains are ideal for applications requiring transparency and openness.
- **Private Blockchain :** Private blockchains are restricted to a specific group of participants. They offer controlled access and are typically used by enterprises for internal operations. Examples include Hyperledger and R3 Corda.

- **Consortium Blockchain :** Consortium blockchains are governed by a group of organizations rather than a single entity. They are semi-decentralized and suitable for industries requiring collaboration, such as supply chain management.
- **Hybrid Blockchain :** Hybrid blockchains combine features of public and private blockchains. They allow organizations to control access while retaining transparency for specific activities.

1.5 NEED FOR AUDITING

Auditing is a crucial process in healthcare to ensure that Electronic Health Records (EHRs) are accurate, secure, and have not been tampered with. In the context of EHRs, auditing involves tracking every interaction with a medical record, including who accessed the data, when, and what changes were made. This helps ensure the accuracy of the records and provides accountability in case of any disputes or discrepancies [11] [13].

Auditing is particularly important in blockchain-based healthcare systems, where the immutability of data is a key feature. However, while blockchain ensures that records cannot be altered, it does not provide a straightforward way to track the reasons behind specific changes. Implementing an effective auditing mechanism alongside blockchain technology is crucial to maintaining the transparency and reliability of healthcare data [5] [10].

Audits also play a vital role in ensuring compliance with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), which mandate the protection and confidentiality of patient information [2] [14]. Regular audits can help identify security vulnerabilities, prevent unauthorized access, and detect any unusual patterns that may indicate malicious activity.

1.6 PROVENANCE IN HEALTHCARE

In healthcare, provenance refers to the detailed record of the history of a healthcare dataset, documenting its origin, modifications, and access throughout its lifecycle. Provenance is essential for ensuring the authenticity and reliability of medical records. It provides a transparent trail of who accessed or modified a patient's data, which is crucial for verifying the integrity of the information [4] [2].

Provenance ensures accountability by making it possible to track any unauthorized changes or tampering with patient records. It acts as an audit trail, enhancing trust in the system by allowing healthcare providers to review the history of any changes to the patient's medical data [16] [13]. This level of transparency is especially important in healthcare where the accuracy of data directly impacts patient safety and treatment decisions [10].

1.7 ORGANIZATION OF THE REPORT

This report is organized into 6 chapters, describing each part of the project with detailed illustrations and system design diagrams.

CHAPTER 2: Literature Review reviews existing research, studies, and relevant literature related to Provenance Aware Verification and Auditing of Electronic Health Record. It discusses the background, theories, and methodologies used by other researchers.

CHAPTER 3: System Design describes the design of the project. It explains the architecture, components, algorithms, and any other technical details.

CHAPTER 4: Implementation provides details about how the project was implemented. It discusses the tools, technologies, programming languages, and frameworks used.

CHAPTER 5: Results and Analysis presents the results of the project. It analyzes the outcomes, compares them with expectations, and discusses any challenges faced during implementation.

CHAPTER 6: Conclusions and Future Work summarizes the findings and draws conclusions. It discusses the significance of the work and its implications.

CHAPTER 2

LITERATURE SURVEY

2.1 OVERVIEW

The reviewed literature highlights the growing potential of blockchain technology in addressing several pressing concerns in the management of healthcare information, including issues related to data isolation, security, interoperability, and provenance. Blockchain has been increasingly explored as a solution to improve the management of Electronic Health Records (EHRs) and facilitate Health Information Exchange (HIE). Key benefits associated with blockchain-based systems include decentralized storage, enhanced security, increased transparency, and better traceability of health data. Despite its promising advantages, the adoption of blockchain in healthcare is accompanied by challenges such as scalability, real-time access to data, and the integration with existing healthcare infrastructures. This literature survey focuses on studies that have explored blockchain for secure, private, and integrity-preserving healthcare data management, with an emphasis on provenance. This section categorizes these works based on their implementation strategies, compares key characteristics, and highlights common pitfalls, thereby pointing out research gaps and opportunities for improvement.

2.2 EHR SHARING AND ACCESS CONTROL

Ensuring privacy and secure access control for EHR sharing remains a core focus of blockchain applications in healthcare. Consortium blockchain models explored by Ramzan et al. prioritized privacy preservation in collaborative EHR sharing [3]. Furthermore, Hong et al. proposed secure access control mechanisms tailored for consumer Internet of Medical Things (IoMT) devices, addressing data security concerns in interconnected ecosystems[14].

Advanced cryptographic techniques, such as Publicly Verifiable Searchable Encryption (PVSE) presented by Wang et al. enabled efficient data retrieval in cloud-assisted healthcare systems [13]. Similarly, the work done by Gohar et al. introduced a secure updatable storage access control system, facilitating real-time updates while preserving data confidentiality [15]. These solutions underline the role of blockchain in addressing critical privacy concerns in EHR sharing.

2.3 BLOCKCHAIN FOR SECURE EHR MANAGEMENT

The integration of blockchain technology into Electronic Health Record (EHR) management has revolutionized data security, accessibility, and transparency. Multiple approaches leverage blockchain's immutable ledger to address challenges in EHR integrity and interoperability. A provenance-focused framework for healthcare data was introduced by Margheri et al. emphasizing traceability to mitigate unauthorized alterations [4]. A systematic review of blockchain-based EHR systems proposed by Shah and Khan analyzed current technologies and highlighted future research needs, such as scalability and consensus efficiency [2]. Furthermore, a novel token-based Pure Proof-of-Stake (PPoS) methodology proposed by Benaich et al. fortified the security infrastructure by combining cryptographic safeguards with efficient consensus mechanisms [5] .

For cloud-hosted medical data, Li et al. proposed a privacy-preserving auditing protocol, enabling verifiable and secure access [17] . Public auditing solutions tailored for decentralized systems were elaborated by Chen et al. integrating dynamic update capabilities with functional commitments to ensure robust data governance [18]. Wang et al. extended these ideas, proposing multi-copy data integrity protocols to handle decentralized storage challenges effectively [13]. These contributions underscore blockchain's role in enhancing healthcare data integrity and traceability.

2.4 PATIENT-CENTRIC DATA EXCHANGE

Empowering patients with control over their medical data while ensuring seamless data exchange across stakeholders is central to blockchain's adoption in healthcare. Blockchain-enabled health information exchange frameworks, such as those discussed by Zhuang et al. and Kumar et al. prioritize patient ownership while ensuring compliance with interoperability standards [19] [12]. Zhang et al. proposed a semantic reference architecture, combining blockchain, IoT, and cloud technologies for enhanced health data interchangeability [20].

Research carried out by Haddad et al. explored challenges associated with secondary EHR utilization, identified a need for secure sharing mechanisms that align with patient privacy and data usage policies [7]. Prototypes examined by Wang et al. underscored the real-world implications of blockchain for healthcare data management, emphasizing user-centric design and operational scalability [6]. These frameworks pave the way for a unified approach to healthcare data exchange and patient empowerment.

2.5 BLOCKCHAIN-DRIVEN INSURANCE AND AUDITING

The application of blockchain in healthcare insurance and data auditing has emerged as a pivotal development. ChainSure, detailed by Karmakar et al. eliminated intermediaries by introducing a blockchain-enabled agent-free insurance system, streamlining claim validation [16]. Public auditing protocols designed for blockchain systems, such as those proposed by Shu et al. and Zhang et al. emphasized secure deduplication to ensure data reliability and optimize storage [10] [20].

Additionally, Chen et al. proposed an innovative auditing framework for shared EHR databases, addressing data privacy concerns while supporting dynamic updates [18]. In work proposed by Miao et al. shared integrity auditing and de-duplication mechanisms demonstrated the feasibility of scalable and reliable blockchain storage solutions [11]. Together, these studies showcased blockchain's transformative role in enhancing healthcare data verifiability and trust.

2.6 FRAMEWORKS FOR BLOCKCHAIN

Building scalable and interoperable frameworks for blockchain-based healthcare systems remains a significant challenge. Studies conducted by Wang et al. and Hong et al. dissected existing frameworks, identifying critical roadblocks in user adoption, system scalability, and standardization [6][14]. Consortium blockchain models proposed by Ramzan et al. balanced security and performance, enabling secure cloud-assisted EHR sharing[3].

Motivations and implementation challenges highlighted by Hong et al. underscore the need for universal standards, robust governance models, and enhanced user education to achieve widespread adoption[14]. Future research must address these issues to ensure that blockchain technology meets the nuanced requirements of healthcare ecosystems.

2.7 PROVENANCE IN HEALTHCARE SYSTEMS

Dynamic provenance mechanisms are critical for maintaining an auditable trail of healthcare data modifications. Studies conducted by authors such as Margheri et al. and Miao et al. have explored decentralized provenance systems, enabling secure tracking of data history without compromising performance. These systems emphasize real-time tracking, ensuring every data modification is recorded on the blockchain [4] [11].

Decentralized provenance frameworks integrate well with collaborative environments, particularly those involving multiple stakeholders, such as hospitals, insurers, and patients. The advancements detailed by Chen et al. illustrate the potential of these systems to achieve real-time, verifiable, and trustworthy data histories, significantly enhancing operational transparency in healthcare [18].

2.8 AI AND BLOCKCHAIN IN HEALTHCARE

The convergence of Artificial Intelligence (AI) and blockchain has opened new possibilities for healthcare data management. A systematic review conducted by Su et al. outlined how AI algorithms integrated with blockchain frameworks enhance decision-making, predictive analytics, and automated auditing [8]. Real-world prototypes explored by Wang et al. demonstrated practical implementations of AI-driven insights within decentralized systems, showcasing their potential to address complex healthcare challenges [6].

These synergistic systems leverage blockchain's transparency and security with AI's analytical capabilities to advance personalized medicine, automate claims processing, and refine diagnostic accuracy.

2.9 SUMMARY OF EXISTING WORK

The literature review comprehensively explores the transformative potential of blockchain in healthcare systems by discussing its applications in EHR management, patient data exchange, insurance systems, privacy preservation, and AI integration. The immutable ledger of blockchain technology makes data more secure, transparent, and interoperable while giving patients the right to control their medical records, with safe and efficient sharing of data. Advanced cryptographic methods and decentralized architectures tackle essential problems in privacy, access control, and data integrity. Besides, blockchain's hybrid nature with AI enables the usage of predictive analytics, personalized medicine, and automation of processes in healthcare.

Though these developments are encouraging, there are still problems associated with blockchain's applicability to healthcare, such as scalability, interoperability, and governance. Dynamic provenance systems and innovative consensus mechanisms provide solutions for tracking real-time data and providing transparency in operations. Future horizons include the incorporation of advanced technologies such as zero-knowledge proofs and sharding to address scalability and privacy. If these challenges are addressed by collaboration among stakeholders and development of robust frameworks, then blockchain can redefine healthcare in a secure, patient-centric ecosystem that will provide for efficient, transparent, and equitable access to medical services.

2.10 OBJECTIVES OF PROPOSED SYSTEM

- To migrate from on-chain blockchain storage to off-chain storage to reduce storage overhead by using distributed file storage systems such as Inter Planetary File System (IPFS).
- To implement a publicly implementable blockchain system to ensure user verifiability.
- To apply a decentralized authorization mechanism in blockchain to improving privacy and security of the users.
- To conduct auditing in blockchain which ensures compliance with standards of the health records.
- To track transactions in blockchain from the creation of a block to track provenance in the system.
- To develop a system which can track provenance, conduct auditing and perform decentralized authorization in blockchain.

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 ARCHITECTURE OF PAVE SYSTEM

The Provenance Aware Verification and Auditing in Blockchain based EHR system (PAVE) depicted in the diagram is a solution for managing sensitive medical data securely, transparently, and efficiently.

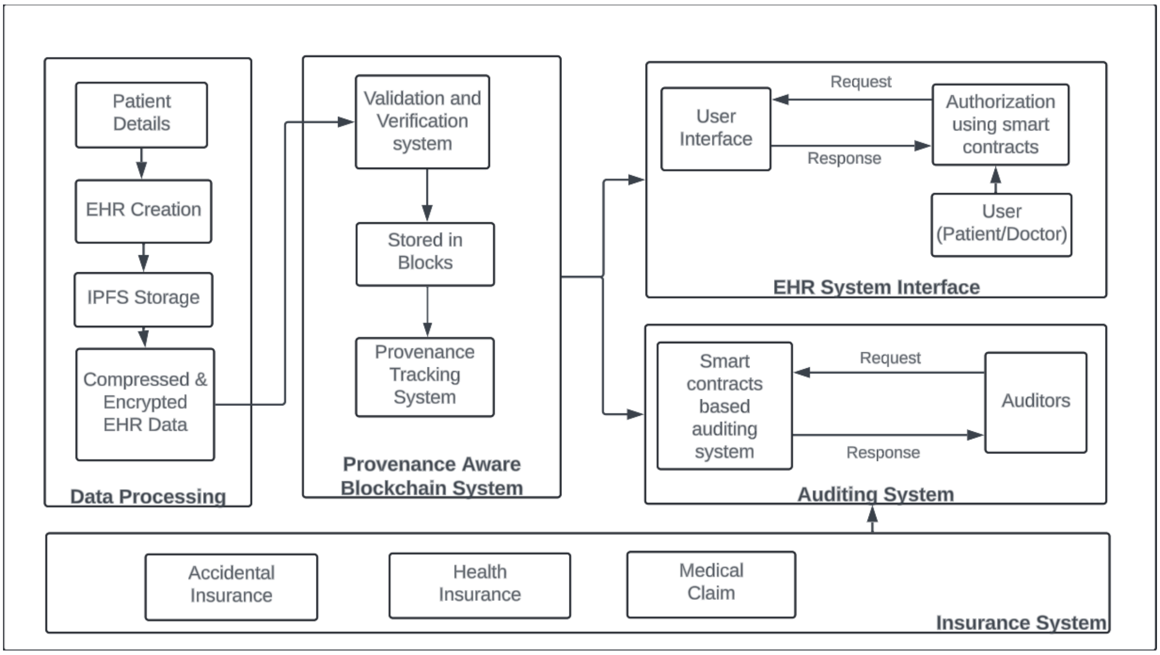


Figure 3.1: Architecture of PAVE System

3.2 DATA PROCESSING MODULE

The Data Processing module is the foundation of the system, handling the initial creation, encryption, and storage of electronic health records (EHRs).

3.2.1 Patient Details

This component collects and organizes raw medical and demographic data provided by patients. It includes personal identification information, medical history, ongoing treatments, test results, and other pertinent details that form the basis of the EHR. This data is sourced directly from healthcare providers or patients themselves during registration.

3.2.2 EHR Creation

Once the patient details are gathered, this component structures the data into a digital format compatible with the system. The EHR is designed to be comprehensive and standardized, ensuring interoperability across various healthcare institutions. This step ensures that the EHR data is consistent, usable, and ready for secure processing.

3.2.3 IPFS Storage

The Inter Planetary File System (IPFS) is utilized for decentralized storage of the EHR. Unlike traditional cloud systems, IPFS provides content-addressable storage by generating a unique hash for every file. This ensures that the EHR cannot be tampered with, as any alteration would result in a new hash. Additionally, the distributed nature of IPFS enhances data availability and reduces risks associated with centralized storage breaches.

3.2.4 Compressed Encrypted EHR Data

To optimize storage and safeguard privacy, EHR data is compressed to reduce its size and encrypted using robust cryptographic techniques. This ensures that sensitive patient information remains protected, even in a distributed environment like IPFS. Encryption also guarantees that only authorized parties can access the data, maintaining patient confidentiality.

3.3 PROVENANCE-AWARE SYSTEM

This module forms the core of the architecture, providing a secure and immutable ledger for managing EHRs. It integrates provenance tracking to ensure accountability.

3.3.1 Validation and Verification System

Before any data is added to the blockchain, it undergoes a strict validation process to ensure its accuracy, integrity, and authenticity. This system checks for tampering, duplicates, and compliance with predefined standards, such as Fast Healthcare Interoperability Resources (FHIR) or Health Level 7 (HL7) protocols. Only verified records are allowed to proceed, minimizing the risk of fraudulent or erroneous data.

3.3.2 Stored in Blocks

After validation, the encrypted EHR data and its associated metadata (e.g., IPFS hash, timestamps, access permissions) are stored in the blockchain as part of sequential blocks. Each block is cryptographically linked to its predecessor, creating a tamper-proof chain of records. This immutability is critical for building trust among stakeholders.

3.3.3 Provenance Tracking System

This system maintains a detailed history of the EHR, including its creation, updates, and access events. Every action is logged on the blockchain, enabling stakeholders to trace the data's origin and verify who accessed or modified it. This feature is vital for regulatory compliance, such as General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA), and for fostering transparency in healthcare processes.

3.4 EHR SYSTEM INTERFACE

The EHR System Interface connects end-users (patients and doctors) to the blockchain system through a user-friendly interface. It manages requests and responses using smart contracts for secure interactions.

- **User Interface:** Patients and doctors access the system through a web or mobile application. Patients can view their medical records, track changes, and control access permissions. Doctors can retrieve patient data, update medical records, and provide diagnoses. The interface is designed to be intuitive, ensuring accessibility for users with varying levels of technical expertise.

- **Authorization using Smart Contracts:** Access to EHRs is governed by smart contracts, which enforce predefined rules for data access and modification. For example, patients may grant or revoke access to their records, while doctors can update medical information only with patient consent. These contracts ensure role-based permissions and eliminate the need for intermediaries, enhancing security and efficiency.

3.5 AUDITING SYSTEM

The auditing system ensures that all actions within the blockchain are monitored and verifiable, fostering trust and accountability.

- **Smart Contracts-Based Auditing System:** This component automatically generates audit trails by analyzing blockchain transaction histories. It records every access or modification event, along with timestamps and user identities, ensuring a comprehensive and immutable log of activities.
- **Auditors:** Independent auditors can review the system's operations to ensure compliance with regulatory standards and detect anomalies. For example, auditors may investigate unauthorized access attempts or validate data integrity. They can request specific audit reports through the interface, which are generated by the smart contracts and backed by blockchain data.

3.6 INTEGRATION WITH INSURANCE COMPANIES

The system's design includes seamless collaboration with insurance companies for claim verification and processing.

- **Insurance Entities (Accidental, Health, Medical Claim):** These entities rely on EHRs to validate insurance claims. The blockchain's immutability ensures that the data shared with insurers is accurate and trustworthy. Insurance companies can request specific EHRs via the system, and the patient or doctor grants access through a smart contract. These streamlines claim approval and minimize fraud, as insurers can independently verify the data's authenticity.

3.7 HARDWARE REQUIREMENTS

- **Processor**: Intel i5 or above.
- **RAM:** 8 GB (minimum)
- **Storage:** SSD with at least 10 GB of free space

3.8 SOFTWARE REQUIREMENTS

- **Ethereum:** Ethereum network (testnet)
- **Ganache:** For local Ethereum blockchain testing and development.
- **Truffle:** For smart contract development, testing, and deployment.
- **Solidity:** Programming language for writing smart contracts.
- **Remix IDE:** Web-based IDE for Solidity contract development and deployment.
- **IPFS:** InterPlanetary File System (IPFS) for decentralized storage of EHR data and medical records. IPFS Desktop or IPFS Cluster can be used for local testing and development.

- **React:** JavaScript library for building the user interface of the web application.
- **Node.js:** JavaScript runtime environment for backend services and npm package management.
- **Web3.js/ethers.js:** JavaScript libraries for interacting with the Ethereum blockchain from the frontend.
- **MetaMask:** Ethereum wallet browser extension for user authentication and transaction signing.

CHAPTER 4

DESIGN AND IMPLEMENTATION

4.1 DATA FLOW DIAGRAM

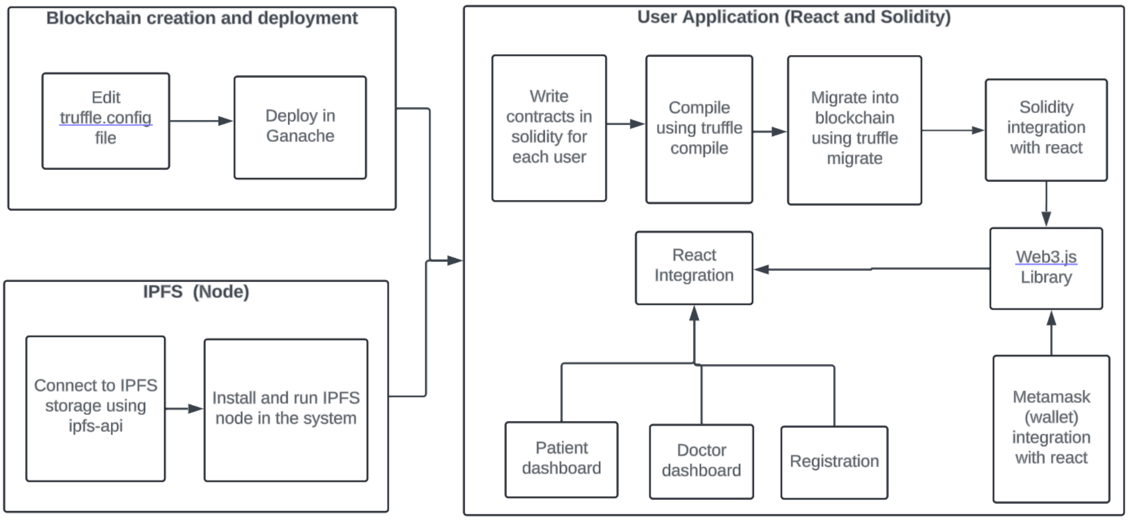

Blockchain creation and deployment
Edit truffle.config file
Deploy in Ganache
IPFS (Node)
Connect to IPFS storage using ipfs-api
Install and run IPFS node in the system
User Application (React and Solidity)
Write contracts in solidity for each user
Compile using truffle compile
Migrate into blockchain using truffle migrate
Solidity integration with react
Web3.js Library
React Integration
Metamask (wallet) integration with react
Patient dashboard
Doctor dashboard
Registration

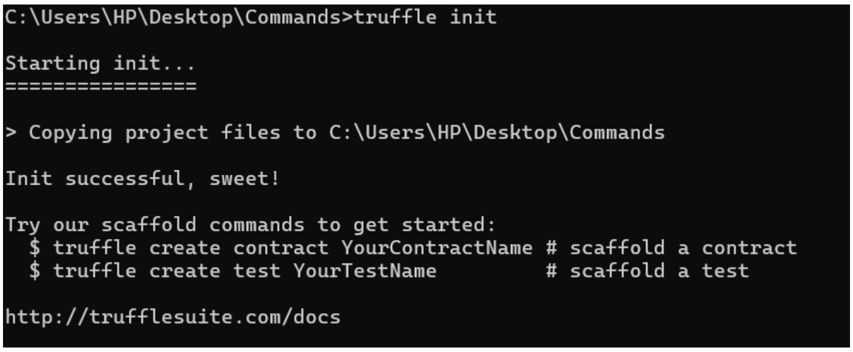
Figure 4.1: Data flow diagram of PAVE System

A Data Flow Diagram (DFD) visually represents the flow of data within a system, showcasing how data is processed, stored, and transferred between entities, processes, and data stores. It provides a high-level overview of the system's functionality, highlighting key inputs, outputs, and interactions, making it ideal for identifying system requirements and data management workflows. Here there are three different data flow blocks such as Blockchain creation and deployment, User Application and the IPFS blocks. The detailed description of each block with its functionality is given below.

4.2 BLOCKCHAIN DEVELOPMENT AND DEPLOYMENT

4.2.1 Initialize the truffle file

Truffle is a React framework library used for smart contract development, deployment and testing purpose. Initializing the truffle file into the project enable to integrate the particular folder with truffle and the ganache environment.

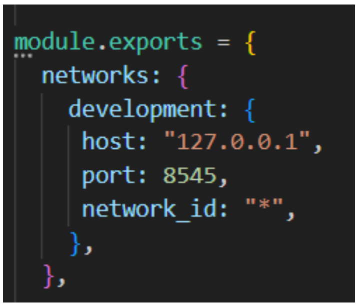


```
C:\Users\HP\Desktop\Commands>truffle init

Starting init...
================

> Copying project files to C:\Users\HP\Desktop\Commands

Init successful, sweet!

Try our scaffold commands to get started:
  $ truffle create contract YourContractName # scaffold a contract
  $ truffle create test YourTestName         # scaffold a test

http://trufflesuite.com/docs
```

Figure 4.2: truffle init

4.2.2 Edit the truffle.config file

Once the truffle is initialized a truffle.config file is automatically formed which contains details about the development network. The truffle-config.js file is edited to configure how the smart contracts shall connect. This configuration should detail the development network like Ganache, port, host, and EVM to match the contracts with settings.

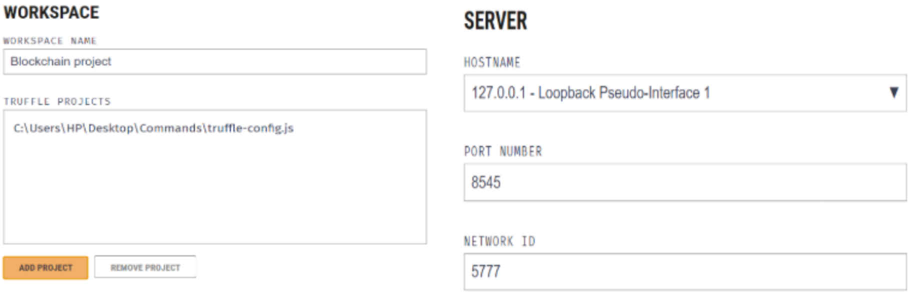


```
module.exports = {
  networks: {
    development: {
     host: "127.0.0.1",
     port: 8545,
     network_id: "*",
    },
  },
```

Figure 4.3: truffle.config file

4.2.3 Deploy in Ganache

Ganache acts as the local Ethereum blockchain for simulating a real blockchain environment, which would be used to test and develop applications. Smart contracts are deployed on Ganache, providing accounts with preloaded Ether, along with an interactive interface to track transactions.



WORKSPACE

WORKSPACE NAME: Blockchain project

TRUFFLE PROJECTS: C:\Users\HP\Desktop\Commands\truffle-config.js

SERVER

HOSTNAME: 127.0.0.1 - Loopback Pseudo-Interface 1

PORT NUMBER: 8545

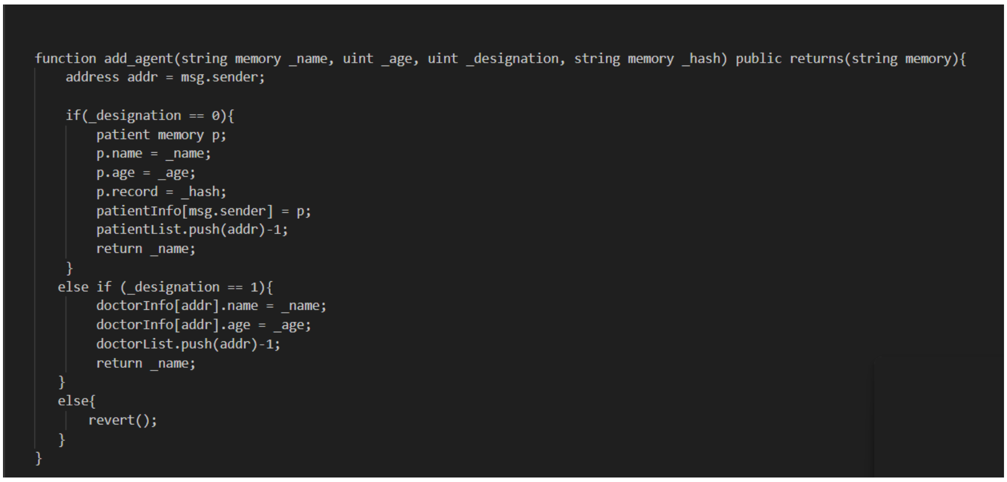
NETWORK ID: 5777

Figure 4.4: Ganache deployment

4.3 USER APPLICATION

4.3.1 Writing contracts in Solidity for each user

Solidity is a programming language designed to write smart contracts for Ethereum framework. Contracts written in Solidity specify the business logic of an application. Every user type has its own functionality-for instance, giving permissions, getting medical records, updating information, etc. It all depends on the specific requirement of the application. Here the contract specifies different users such as doctor and patient.

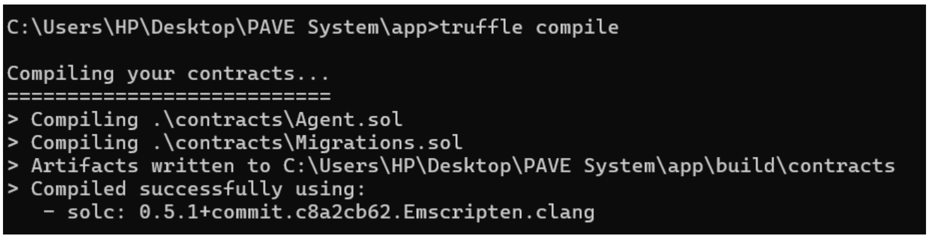


```
function add_agent(string memory _name, uint _age, uint _designation, string memory _hash) public returns(string memory){
    address addr = msg.sender;

    if(_designation == 0){
        patient memory p;
        p.name = _name;
        p.age = _age;
        p.record = _hash;
        patientInfo[msg.sender] = p;
        patientList.push(addr)-1;
        return _name;
    }
   else if (_designation == 1){
        doctorInfo[addr].name = _name;
        doctorInfo[addr].age = _age;
        doctorList.push(addr)-1;
        return _name;
   }
   else{
       revert();
   }
}
```

Figure 4.5: Sample Contract

4.3.2 Compilation

Smart contract written out is compiled in bytecode with their ABI that can be easily deployed and manipulated programmatically from the front end while interacting with this contract. Compilation can be done with truffle compile.

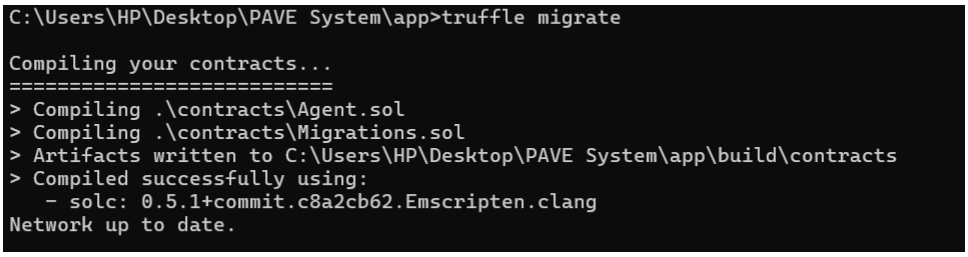


```
C:\Users\HP\Desktop\PAVE System\app>truffle compile

Compiling your contracts...
===========================
> Compiling .\contracts\Agent.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\HP\Desktop\PAVE System\app\build\contracts
> Compiled successfully using:
   - solc: 0.5.1+commit.c8a2cb62.Emscripten.clang
```

Figure 4.6: Compilation of contract

4.3.3 Migrate to blockchain

Contracts compiled must be migrated to blockchain so that the contracts can be applied to the blockchain environment. Migration script is called to ensure right deployment also initialization of each contract made. Migration to blockchain is done using truffle migrate.

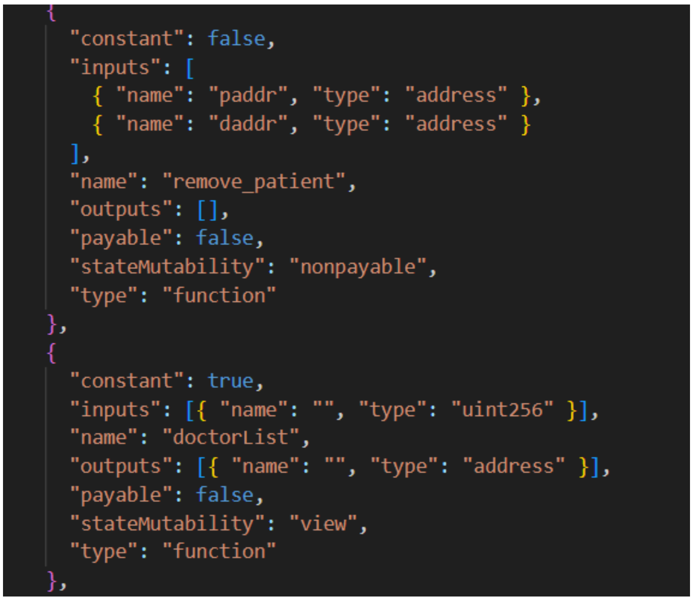


```
C:\Users\HP\Desktop\PAVE System\app>truffle migrate

Compiling your contracts...
===========================
> Compiling .\contracts\Agent.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\HP\Desktop\PAVE System\app\build\contracts
> Compiled successfully using:
   - solc: 0.5.1+commit.c8a2cb62.Emscripten.clang
Network up to date.
```

Figure 4.7: Migration to blockchain

4.3.4 Integration between Solidity and React

After deployment, the contracts are connected to the React frontend. This is done by loading the Application Binary Interface (ABI) and contract addresses into Web3.js, allowing interaction between the frontend and blockchain.

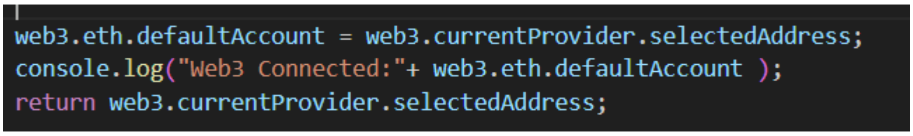


```
{
  "constant": false,
  "inputs": [
    { "name": "paddr", "type": "address" },
    { "name": "daddr", "type": "address" }
  ],
  "name": "remove_patient",
  "outputs": [],
  "payable": false,
  "stateMutability": "nonpayable",
  "type": "function"
},
{
  "constant": true,
  "inputs": [{ "name": "", "type": "uint256" }],
  "name": "doctorList",
  "outputs": [{ "name": "", "type": "address" }],
  "payable": false,
  "stateMutability": "view",
  "type": "function"
},
```

Figure 4.8: Sample ABI

4.3.5 Web3.js Library

Web3.js is used as a bridge between the React frontend and the Ethereum blockchain. It is utilized to send transactions, read data from contracts, and manage user accounts through MetaMask.

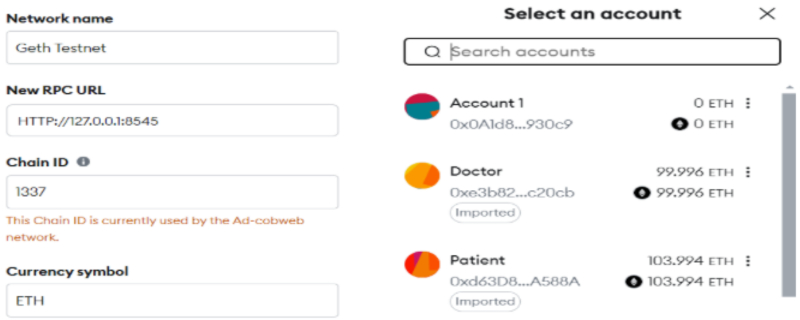


```
web3.eth.defaultAccount = web3.currentProvider.selectedAddress;
console.log("Web3 Connected:"+ web3.eth.defaultAccount );
return web3.currentProvider.selectedAddress;
```

Figure 4.9: Web3 Initialization

4.3.6 MetaMask (wallet) integration with React

MetaMask, the browser extension wallet, has been integrated into the application so that users can interact with the blockchain. Users authenticate and sign transactions using their MetaMask accounts.



Network name

Geth Testnet

New RPC URL

HTTP://127.0.0.1:8545

Chain ID

1337

This Chain ID is currently used by the Ad-cobweb network.

Currency symbol

ETH

Select an account

Search accounts

Account 1
0x0A1d8...930c9
0 ETH
0 ETH

Doctor
0xe3b82...c20cb
Imported
99.996 ETH
99.996 ETH

Patient
0xd63D8...A588A
Imported
103.994 ETH
103.994 ETH

Figure 4.10: MetaMask Connection

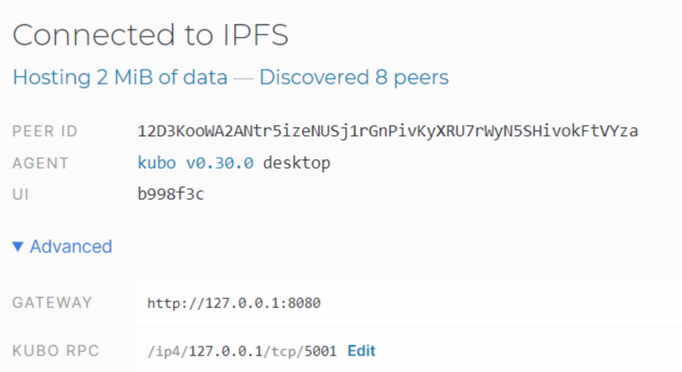
4.3.7 React Integration

- **Patient Dashboard:** This provides the patients with the possibility of viewing their medical records and controlling access permissions.
- **Doctor Dashboard:** This helps doctors view and update the medical records of patients, and upload diagnosis details.
- **Registration:** The functionality is to register the account of new users in the system. Their information saves securely in the blockchain.

4.4 INTER PLANETART FILE SYSTEM (NODE)

4.4.1 IPFS node installation and execution

An Inter Planetary File System node is a distributed peer-to-peer file storage system which uses hash tables.It is installed and set up on the local machine. This node is used to store and retrieve files (e.g., medical images) in a decentralized manner.



Connected to IPFS

Hosting 2 MiB of data — Discovered 8 peers

PEER ID	12D3KooWA2ANtr5izeNUSj1rGnPivKyXRU7rWyN5SHivokFtVYza
AGENT	kubo v0.30.0 desktop
UI	b998f3c

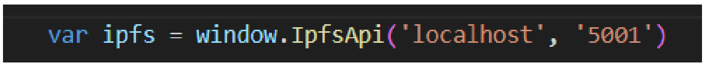
▼ Advanced

GATEWAY	http://127.0.0.1:8080
KUBO RPC	/ip4/127.0.0.1/tcp/5001 Edit

Figure 4.11: IPFS Setup

4.4.2 Connection to IPFS storage using ipfs-api

The React application connects to the IPFS node using the ipfs-http-client library. This allows the app to upload files to the IPFS network, retrieve files by their hash, and manage decentralized storage operations seamlessly.



```
var ipfs = window.IpfsApi('localhost', '5001')
```

Figure 4.12: IPFS API

4.5 SOLIDITY CONTRACT FOR PAVE SYSTEM

The **patient side** of the smart contract allows a user to register as a patient through the `add_agent` function by providing their name, age, and a medical record hash. Once registered, patients can grant access to their medical records to doctors by using the `permit_access` function, which requires a payment of 2 ether. This function adds the doctor's address to the patient's `doctorAccessList` and vice versa, enabling both parties to interact with the patient's data. Patients can also revoke access to a doctor using the `revoke_access` function, which removes the doctor's access and refunds the 2 ether. The `get_patient` function allows retrieval of a patient's personal information, including their medical history and record, while the `get_patient_doctor_name` function enables the retrieval of the associated doctor's name.

The **doctor side** allows a user to register as a doctor using the `add_agent` function, which requires the doctor's name and age. Doctors are compensated 2 ether when updating an patient's diagnosis via the `diagnosis_claim` function. The function checks if the doctor has access to the patient's records, and upon successful verification, updates the patient's medical record and ensures the doctor is paid. This process ensures that both doctors and patients have distinct roles, with secure and controlled access to medical records, payments, and claims management, all governed by clear access control and transaction rules within the contract.

Algorithm 4.1 Agent Smart Contract (Patient Side)

```
Input Doctor Hash Value
Output Access Grant
Process:
Define Struct patient:
    name (string), age (uint), doctorAccessList (address array),
    diagnosis (uint array), record (string)
Variables:
    patientList (address array), patientInfo (mapping of address to patient struct)
    doctorInfo (mapping of address to doctor struct)
function ADD_AGENT(name, age, designation, hash)
    Get addr as msg.sender
    if designation == 0 then
        Initialize a new patient instance
        Assign name, age, hash to patientInfo[addr]
        Append addr to patientList return name
    else
        Revert (designation must be 0 for patient)
    end if
end function
function GET_PATIENT(addr) return patientInfo[addr] fields (name, age, diagnosis, record)
end function
function GET_PATIENT_DOCTOR_NAME(paddr, daddr) return patientInfo[paddr].name, doctorInfo[daddr].name
end function
function PERMIT_ACCESS(addr)
Require: msg.value == 2 ether
    Add msg.sender to doctorInfo[addr].patientAccessList
    Add addr to patientInfo[msg.sender].doctorAccessList
end function
function REVOKE_ACCESS(daddr)
    Call remove_patient(msg.sender, daddr)
    Transfer 2 ether to msg.sender
end function
function REMOVE_PATIENT(paddr, daddr)
    Remove paddr from doctorInfo[daddr].patientAccessList
    Remove daddr from patientInfo[paddr].doctorAccessList
end function
```

Algorithm 4.2 Agent Smart Contract (Doctor Side)

```
Input Patient Hash Value
Output Patient Diagnosis
Process:
Define Struct doctor:
    name (string), age (uint), patientAccessList (address array)
Variables:
    doctorList (address array), doctorInfo (mapping of address to doctor struct)
    patientInfo (mapping of address to patient struct)
function ADD_AGENT(name, age, designation)
    Get addr as msg.sender
    if designation == 1 then
        Assign name, age to doctorInfo[addr]
        Append addr to doctorList return name
    else
        Revert (designation must be 1 for doctor)
    end if
end function
function GET_DOCTOR(addr) return doctorInfo[addr] fields (name, age)
end function
function PERMIT_ACCESS(addr)
Require: msg.value == 2 ether
    Add msg.sender to doctorInfo[addr].patientAccessList
    Add addr to patientInfo[msg.sender].doctorAccessList
end function
function DIAGNOSIS_CLAIM(paddr, diagnosis, hash)
    Check if paddr exists in doctorInfo[msg.sender].patientAccessList
    if True then
        Transfer 2 ether to msg.sender
        Set patientInfo[paddr].record = hash
        Call remove_patient(paddr, msg.sender)
    else
        Revert (paddr not found in patient list)
    end if
end function
function REMOVE_PATIENT(paddr, daddr)
    Remove paddr from doctorInfo[daddr].patientAccessList
    Remove daddr from patientInfo[paddr].doctorAccessList
end function
```

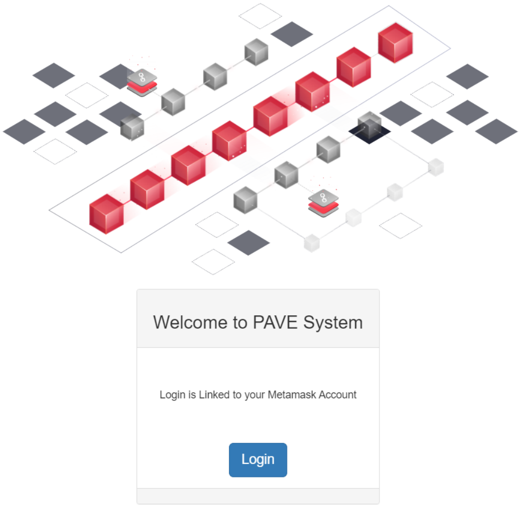
CHAPTER 5

RESULTS AND PERFORMANCE ANALYSIS

This chapter contains the results obtained and the related analysis with the related works carried out.

5.1 REGISTRATION PAGE

The registration page registers each user as either patient or doctor. The functionality is to register the account of new users in the system. Their information saves securely in the blockchain Fig 5.1 depicts the Registration Page of PAVE System.



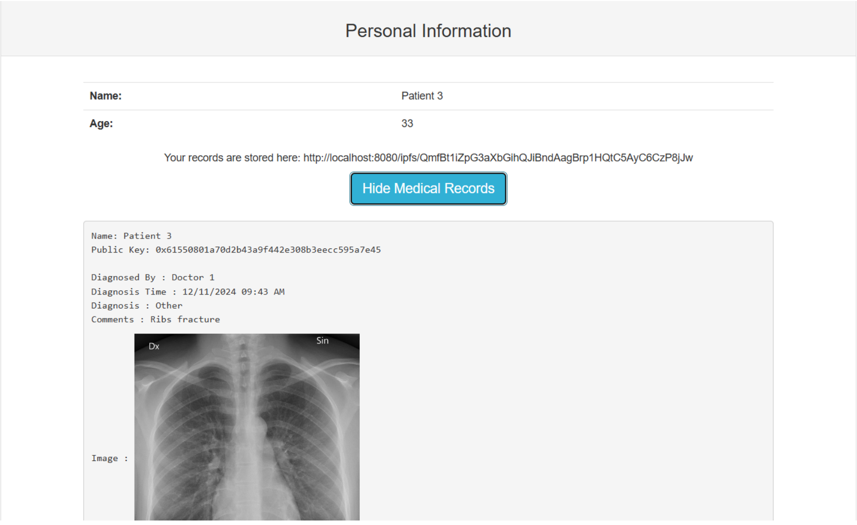
Welcome to PAVE System

Login is Linked to your Metamask Account

Figure 5.1: Registration Page of PAVE System

5.2 PATIENT DASHBOARD

The patient dashboard efficiently displays all the details that a patient can achieve through the blockchain application. The patient's personal details, their medical records and a dashboard where they can give access to their medical records to particular doctor is available in Fig 5.2 and Fig 5.3.



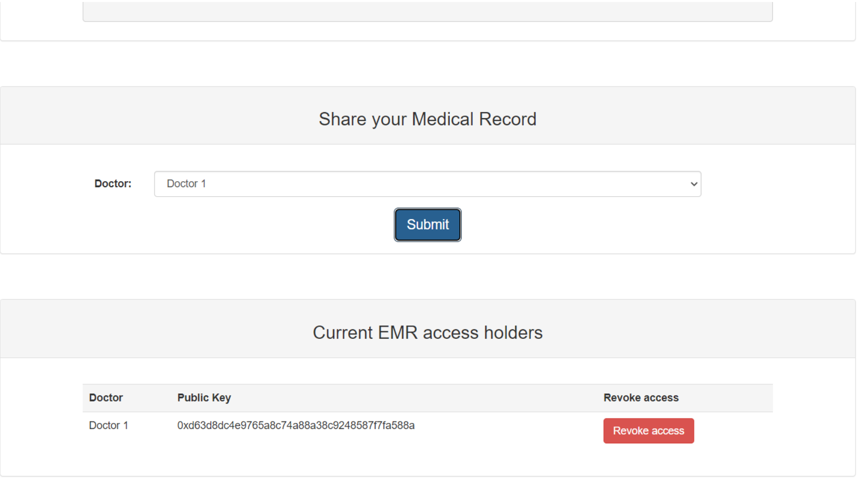
Personal Information

Name:	Patient 3
Age:	33

Your records are stored here: http://localhost:8080/ipfs/QmfBt1iZpG3aXbGihQJiBndAagBrp1HQtC5AyC6CzP8jJw

```
Name: Patient 3
Public Key: 0x61550801a70d2b43a9f442e308b3eecc595a7e45

Diagnosed By : Doctor 1
Diagnosis Time : 12/11/2024 09:43 AM
Diagnosis : Other
Comments : Ribs fracture
Image :
```

Figure 5.2: Patient Dashboard 1



Share your Medical Record

Doctor: Doctor 1

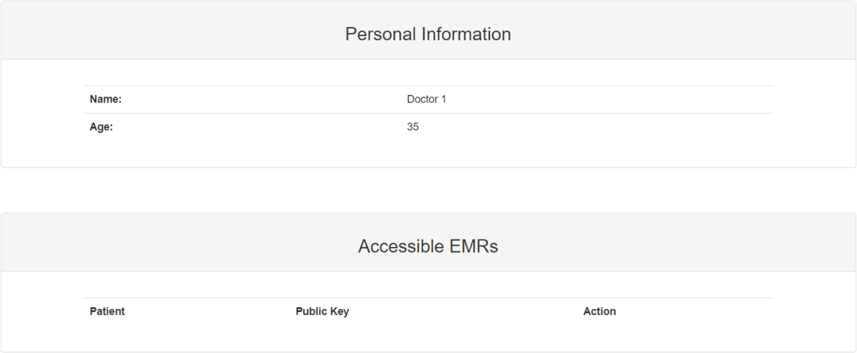
Current EMR access holders

Doctor	Public Key	Revoke access
Doctor 1	0xd63d8dc4e9765a8c74a88a38c9248587f7fa588a	Revoke access

Figure 5.3: Patient Dashboard 2

5.3 DOCTOR DASHBOARD

The doctor's dashboard contains details about the personal details of doctor, then the accessible EHR list form where the doctor can update the details. The doctor can diagnose the patient and add the details of the diagnosis , they can also add image to the diagnosis and also state if the patient is eligible for insurance or not, this is depicted in Fig 5.4 and Fig 5.5.



Personal Information

Name:	Doctor 1
Age:	35

Accessible EMRs

Patient	Public Key	Action

Figure 5.4: Doctor Dashboard 1

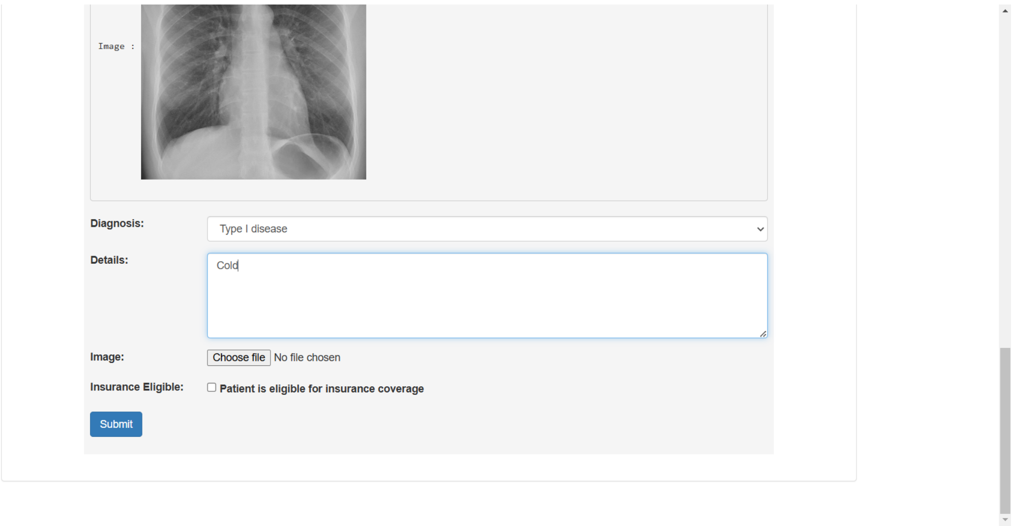


Image :

Diagnosis: Type I disease

Details: Cold

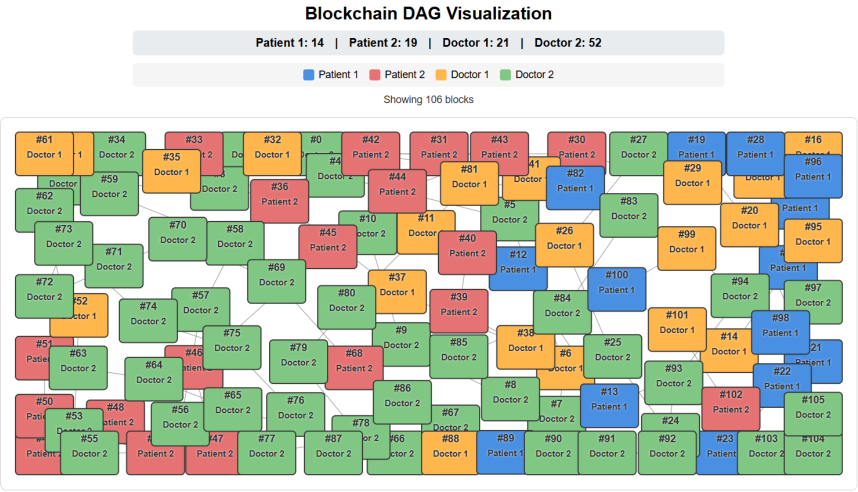
Image: Choose file No file chosen

Insurance Eligible: □ Patient is eligible for insurance coverage

Figure 5.5: Doctor Dashboard 2

5.4 BLOCKS IN PAVE SYSTEM

The number of blocks created in a local ganache environment through the course of this project with auto mining is given below in Fig 5.6. Each block in blockchain is associated with each user in the blockchain system. Each different color in the DAG structure represents each different user. With The blockchain with the latest 40 block is as given below in Fig 5.7.



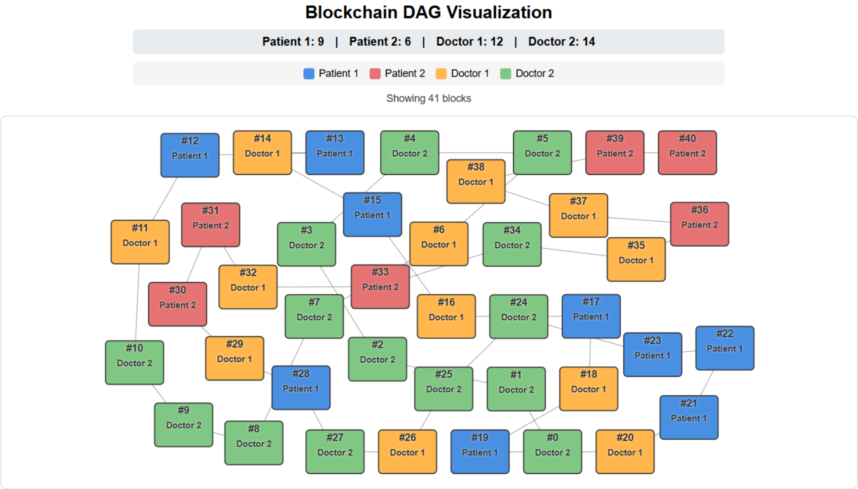
Blockchain DAG Visualization

Patient 1: 14 | Patient 2: 19 | Doctor 1: 21 | Doctor 2: 52

🟦 Patient 1 🟥 Patient 2 🟧 Doctor 1 🟩 Doctor 2

Showing 106 blocks

Figure 5.6: Total Blocks in Blockchain



Blockchain DAG Visualization

Patient 1: 9 | Patient 2: 6 | Doctor 1: 12 | Doctor 2: 14

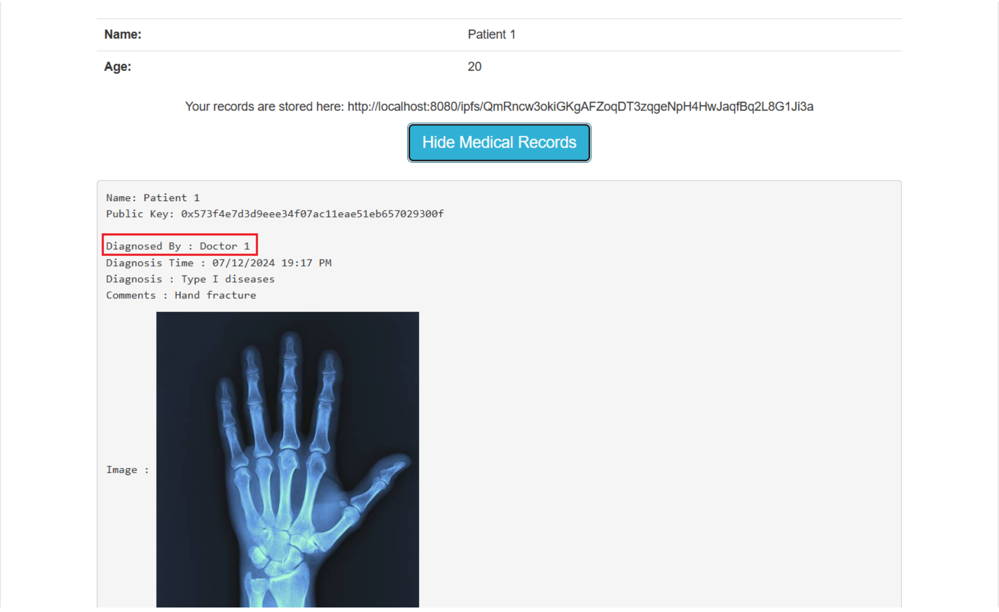
🟦 Patient 1 🟥 Patient 2 🟧 Doctor 1 🟩 Doctor 2

Showing 41 blocks

Figure 5.7: Latest Blocks in Blockchain

5.5 STORAGE IN BLOCKS

The blocks in the PAVE system contains the hashes of all the dats stored in the distributed storage system (IPFS). These datas are stored in the hash of the patient record. Each patient can give access to any doctors in the system, and the doctors can add diagnosis to the patient record. Fig 5.8 and Fig 5.9 gives the details of the patient diagnosis data available in the patient dashboard.

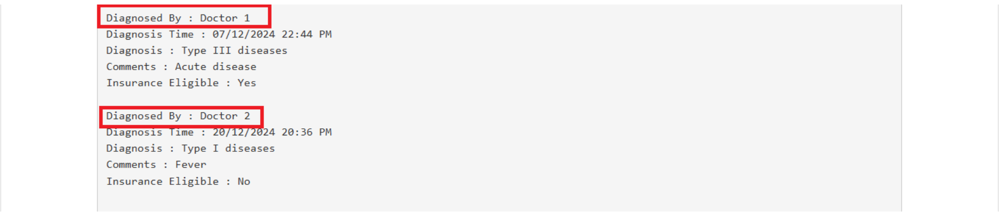


Name:	Patient 1
Age:	20

Your records are stored here: http://localhost:8080/ipfs/QmRncw3okiGKgAFZoqDT3zqgeNpH4HwJaqfBq2L8G1Ji3a

```
Name: Patient 1
Public Key: 0x573f4e7d3d9eee34f07ac11eae51eb657029300f

Diagnosed By : Doctor 1
Diagnosis Time : 07/12/2024 19:17 PM
Diagnosis : Type I diseases
Comments : Hand fracture

Image :
```

Figure 5.8: Patient Data 1

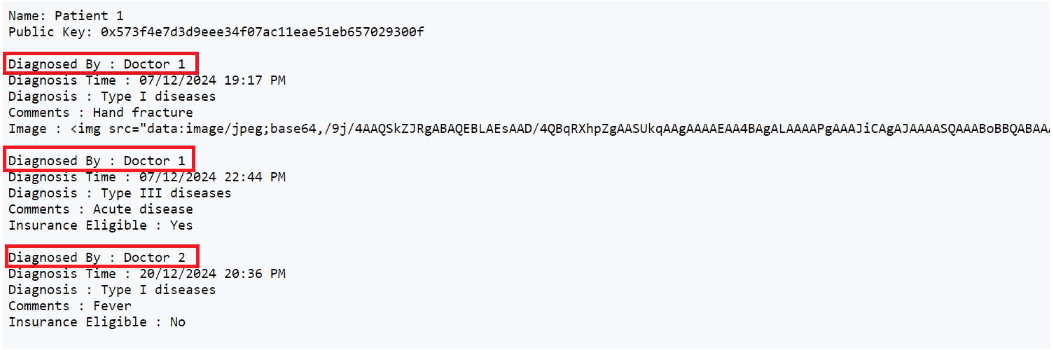


```
Diagnosed By : Doctor 1
Diagnosis Time : 07/12/2024 22:44 PM
Diagnosis : Type III diseases
Comments : Acute disease
Insurance Eligible : Yes

Diagnosed By : Doctor 2
Diagnosis Time : 20/12/2024 20:36 PM
Diagnosis : Type I diseases
Comments : Fever
Insurance Eligible : No
```

Figure 5.9: Patient Data 2

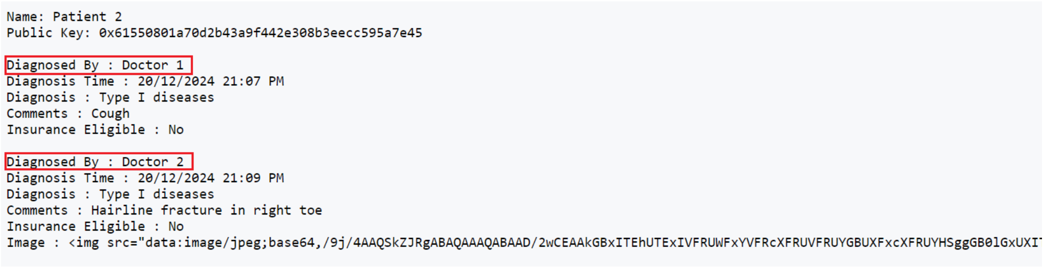
5.6 PATIENT DATA IN IPFS

Similarly the patient data in the IPFS contains the following information stored under the has value. Fig 5.10 and Fig 5.11 shows the details in the IPFS system. This shows that each patient can give access to their medical records to more than one doctors. Fig 5.10 gives the details of diagnosis stored for Patient 1 and Fig 5.11 gives details of diagnosis stored for Patient 2.



```
Name: Patient 1
Public Key: 0x573f4e7d3d9eee34f07ac11eae51eb657029300f

Diagnosed By : Doctor 1
Diagnosis Time : 07/12/2024 19:17 PM
Diagnosis : Type I diseases
Comments : Hand fracture
Image : <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEBLAEsAAD/4QBqRXhpZgAASUkqAAgAAAAEAA4BAgALAAAAPgAAAJiCAgAJAAAASQAAABoBBQABAA

Diagnosed By : Doctor 1
Diagnosis Time : 07/12/2024 22:44 PM
Diagnosis : Type III diseases
Comments : Acute disease
Insurance Eligible : Yes

Diagnosed By : Doctor 2
Diagnosis Time : 20/12/2024 20:36 PM
Diagnosis : Type I diseases
Comments : Fever
Insurance Eligible : No
```

Figure 5.10: Patient 1 Data



```
Name: Patient 2
Public Key: 0x61550801a70d2b43a9f442e308b3eecc595a7e45

Diagnosed By : Doctor 1
Diagnosis Time : 20/12/2024 21:07 PM
Diagnosis : Type I diseases
Comments : Cough
Insurance Eligible : No

Diagnosed By : Doctor 2
Diagnosis Time : 20/12/2024 21:09 PM
Diagnosis : Type I diseases
Comments : Hairline fracture in right toe
Insurance Eligible : No
Image : <img src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAkGBxITEhUTExIVFRUWFxYVFRcXFRUVFRUYGBUXFxcXFRUYHSggGB0lGxUXI
```

Figure 5.11: Patient 2 Data

5.7 PERFORMANCE ANALYSIS

To analyze the performance of the system the gas consumption details were taken into account. In blockchain, gas price is the price per unit of computation that a participant is willing to pay for a transaction on the network. Gas is a unit of measurement that represents the computational effort required for specific operations. When utilizing the proposed system, patients initially need to register on a primary smart contract. The gas consumption levels are low when compared with the existing system. Gas consuptions are generally represented in Wie. Wei is the smallest unit of Ether, equivalent to 1 quintillionth of an Ether. The gas consumption for contract deployment is 2600 wie. Other consecutive activities like agent call, access grant and revoke consumes a fees of around 2 ether which is the lowest possible gas fees.

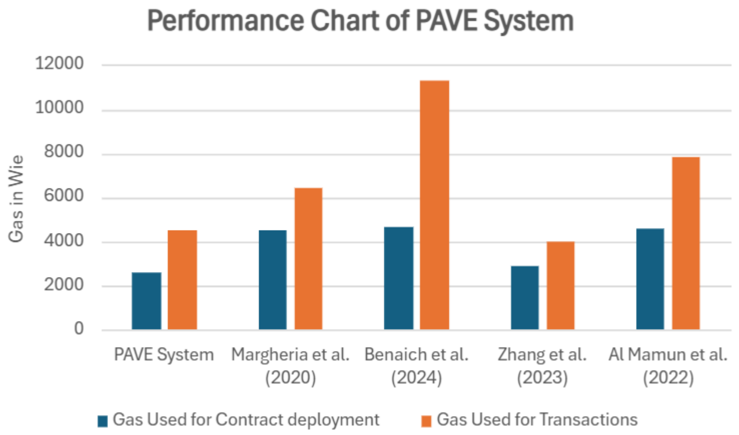


Figure 5.12: Performance Chart

Table 5.1: Existing system v/s proposed system

Feature	**margheri2020**	**benaich2024**	**zhang2023**	**al2022**	**PAVE System**
Blockchain Implementation	Private	Private	Consortium	Private	Public
Storage Implementation	On-Chain	On-Chain	Cloud	Cloud	Off-Chain
Authorization Mechanism	No	Yes	No	No	Yes
Provenance Tracking	No	No	No	No	Yes

5.8 CHALLENGES IN IMPLEMENTATION

The PAVE system is a patient-centric EHR sharing system which gives the patient full athority to share their medical records with the doctors. PAVE system is implemented in a public blockchain (Ganache). Implementation in a public blockchain makes it difficult to authenticate the users. While implementing this system the challenges faced were with the addition of more than two actors into the system. The auditors or the insurance claim must be verified and authenticated by more than one user, which is not feasibile in a publically implemented blockchain application. More than two actor interaction requires authenticating each user individually. Rather using a private blockchain such as Hedera network will help in authorizing its users within a given organization without any explicit means. It also introduces a dedicated channel for communication hence improving security. Moreover, using a private blockchain like Hedera also facilitates interoperability between organizations.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 CONCLUSIONS

The proposed blockchain-based healthcare system presents a new way of handling EHRs by ensuring safe, transparent, and patient-centric data control. Through decentralized storage and smart contracts, it enables efficient provenance tracking, thus making it possible to accurately audit medical data access and putting patients in full control of their health records. The system ensures interoperability and gives a smooth exchange of health information. Moreover, the use of blockchain strengthens transparency, simplifies management, and raises trust among patients and healthcare providers. Its decentralized mechanisms further strengthen data integrity with a reliable and efficient framework suited for modern healthcare needs.

This solution will form a foundation for secure and transparent healthcare data management, marking a significant step forward in the healthcare sector. It designs a decentralized system for a patient-centric EHR management. It contains actors like patients and doctors. Patient can have full control over their records and can provide access to doctors for their medical records. Thus ensuring full authority to user. The enabling of blockchain technology ensures transparent and highly reliable service.

6.2 FUTURE WORK

The blockchain-based healthcare system's future work would be based on acquiring the aspects of scalability and performance. It will use a private blockchain infrastructure like Hedera for enhancing transaction throughput, latency, and the efficient manipulation of large-scale healthcare data. Introducing and incorporating advanced consensus mechanisms such as Proof of Authority or Byzantine Fault Tolerance will further boost system efficiency.This can be done with the help of Hedera blockchain infrastructure. Moreover research work is going on with integrating blockchain technology with artificial intelligence to enhance system efficiency to a next level.

REFERENCES

[1] Lianshan Sun, Diandong Liu, Yang Li, and Danni Zhou. A blockchain-based e-healthcare system with provenance awareness. *IEEE Access*, 2024.

[2] Shahid Munir Shah and Rizwan Ahmed Khan. Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*, 8:136947–136965, 2020.

[3] Sadia Ramzan, Aqsa Aqdus, Vinayakumar Ravi, Deepika Koundal, Rashid Amin, and Mohammed A Al Ghamdi. Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management*, 70(8):2874–2890, 2022.

[4] Andrea Margheri, Massimiliano Masi, Abdallah Miladi, Vladimiro Sassone, and Jason Rosenzweig. Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, 141:104197, 2020.

[5] Rihab Benaich, Saida El Mendili, and Youssef Gahi. Securing ehrs with a novel token-based and ppos blockchain methodology. *IEEE Access*, 2024.

[6] Yong Wang, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain. *IEEE Access*, 7:136704–136719, 2019.

[7] Alaa Haddad, Mohamed Hadi Habaebi, Md Rafiqul Islam, Nurul Fadzlin Hasbullah, and Suriza Ahmad Zabidi. Systematic review on ai-blockchain based e-healthcare records management systems. *IEEE Access*, 10:94583–94615, 2022.

[8] Ye Su, Jiameng Sun, Jing Qin, and Jiankun Hu. Publicly verifiable shared dynamic electronic health record databases with functional commitment supporting privacy-preserving integrity auditing. *IEEE Transactions on Cloud Computing*, 10(3):2050–2065, 2020.

[9] Emeka Chukwu and Lalit Garg. A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. *IEEE Access*, 8:21196–21214, 2020.

[10] Jiangang Shu, Xing Zou, Xiaohua Jia, Weizhe Zhang, and Ruitao Xie. Blockchain-based decentralized public auditing for cloud storage. *IEEE Transactions on Cloud Computing*, 10(4):2366–2380, 2021.

[11] Ying Miao, Keke Gai, Liehuang Zhu, Kim-Kwang Raymond Choo, and Jaideep Vaidya. Blockchain-based shared data integrity auditing and deduplication. *IEEE Transactions on Dependable and Secure Computing*, 2023.

[12] R Prasanna Kumar and Showri Rayalu Bandanadam. Block chain-based decentralized public auditing for cloud storage with improved eigamal encryption model. *International Journal of Information Technology*, 16(2):697–711, 2024.

[13] Jingwei Wang, Xinchun Yin, Jianting Ning, Shengmin Xu, Guowen Xu, and Xinyi Huang. Secure updatable storage access control system for ehrs in the cloud. *IEEE Transactions on Services Computing*, 16(4):2939–2953, 2022.

[14] Yujie Hong, Liang Yang, Wei Liang, and Anke Xie. Secure access control for electronic health records in blockchain-enabled consumer internet of medical things. *IEEE Transactions on Consumer Electronics*, 2023.

[15] Ahmad N Gohar, Sayed Abdelgaber Abdelmawgoud, and Marwa Salah Farhan. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and iot. *IEEE Access*, 10:92137–92157, 2022.

[16] Amiya Karmakar, Pritam Ghosh, Partha Sarathi Banerjee, and Debashis De. Chainsure: Agent free insurance system using blockchain for healthcare 4.0. *Intelligent Systems with Applications*, 17:200177, 2023.

[17] Xiong Li, Shanpeng Liu, Rongxing Lu, Muhammad Khurram Khan, Ke Gu, and Xiaosong Zhang. An efficient privacy-preserving public auditing protocol for cloud-based medical storage system. *IEEE Journal of Biomedical and Health Informatics*, 26(5):2020–2031, 2022.

[18] Biwen Chen, Tao Xiang, Debiao He, Hongwei Li, and Kim-Kwang Raymond Choo. Bpvse: Publicly verifiable searchable encryption for cloud-assisted electronic health records. *IEEE Transactions on Information Forensics and Security*, 18:3171–3184, 2023.

[19] Yan Zhuang, Lincoln R Sheets, Yin-Wu Chen, Zon-Yin Shae, Jeffrey JP Tsai, and Chi-Ren Shyu. A patient-centric health information exchange framework using blockchain technology. *IEEE journal of biomedical and health informatics*, 24(8):2169–2176, 2020.

[20] Qingyang Zhang, Dongfang Sui, Jie Cui, Chengjie Gu, and Hong Zhong. Efficient integrity auditing mechanism with secure deduplication for blockchain storage. *IEEE Transactions on Computers*, 72(8):2365–2376, 2023.

[21] Abdullah Al Mamun, Sami Azam, and Clementine Gritti. Blockchain-based electronic health records management: a comprehensive review and future research direction. *IEEE Access*, 10:5768–5789, 2022.