A blockchain-based approach for securing Electronic Hospital Records

MSc Research Project
Cyber Security

Geetesh Vaswani
Student ID: X20194102

School of Computing
National College of Ireland

Supervisor: Mr. Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Geetesh Vaswani		
Student ID:	X20194102		
Programme:	MSc in Cybersecurity	**Year:**	2021-22
Module:	MSc Research Project		
Supervisor:	Mr. Ross Spelman		
Submission Due Date:	15 December 2022		
Project Title:	A blockchain-based approach for securing Electronic Hospital Records		
Word Count:	7254		
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: Geetesh Vaswani

Date: 15 December 2022

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):	

A blockchain-based approach for securing Electronic Hospital Records

Geetesh Vaswani
X20194102

Abstract

Blockchain technology has been widely studied and has been used in various industries to provide benefits such as security, privacy, and decentralization. The healthcare sector can also benefit from blockchain technology, particularly in the area of electronic health records (EHRs). EHR systems often face issues with data security, integrity, and management. This paper includes the advantages, disadvantages and limitations of blockchain in EHR. A blockchain based model has also been proposed and implemented by following the SSDLC methodology. Our model aims to provide secure storage of electronic records through the use of blockchain storage. This framework could provide a scalable, secure, and integral blockchain-based solution for EHR systems.

1 Introduction

Medical records, for decades, have been maintained using traditional paper-based record system in the form of films, discs, papers physically in a storage facility to be fetched when needed. However, with the digital revolution, physical storage is no longer considered as a secure, reliable or an efficient solution for maintaining and sharing any form of information. Electronic Health Records (EHRs) systems were implemented to provide ease of maintenance and wide accessibility of the records by making them digital. EHR systems persist detailed patient information in the form of Electronic Medical Record (EMRs) which can be made available to the medics urgently in time of need. These blockchain based EHR's have been designed to be reliable, efficient and secure by encrypting patient data and reducing maintenance costs.

Digitalization has been on the key items for growth agendas in every nation. Management is taking initiatives to create new policies for healthcare systems and public health such as eHealth Benefits to Ireland which proposes a more personalised citizen-centric healthcare. "It facilitates socio-economic inclusion and equality, quality of life and patient empowerment through greater transparency, access to services and information and the use of social media for health." (European Union eHealth Strategy for Ireland 2012-2020)

However, digitalization without severe security measures can lead to leakage of critical data during sharing and transmission between various involved identities. This interoperability of data is very crucial in the healthcare sector and data is often persisted in a centralized location to allow easy accessibility. Centralization of data provides easy access for both, authorized and unauthorized, users thus making privacy a concern. Data security and privacy are a challenge in the current ways of storing data on centralized servers and data sharing through EHRs.

Higher digitalization with less integration can lead to risk of data leakage, sniffing, cyberattacks. Upon accessing the data, the attacker encrypts the data with the motive of leaking the data unless ransom has been paid in exchange of it. Blockchain provides a possible solution for secure data sharing and storing. It could also benefit by enabling collaborative clinical decision-making in precision medicine. By usage of certification authorities, blockchain MSPs and smart contracts, data security and privacy are achieved in the blockchain.

1.1 Project Background

Medical or health records are defined as a compilation of confidential facts of an individual's health history, which includes their past and present health conditions, a record of the treatments administered, and events affecting the patient. These records form a critical part of the individual's identity as they assist medical professionals to treat a patient but may also be used for other adverse purposes like profiling that may lead to discrimination. Hence, the HIPAA law classifies medical records as Personal Identifiable Information (PII), and is treated with appropriate compliance standards. Traditionally, health records were stored physically which also brought with it the general issues of storing any information in a physical form. Physical records are difficult to share among medical establishments, susceptible to destruction due to natural or man-made disasters, tedious to copy or replicate, and lastly, prone to damage over time. Digitalization of critical records forms an important transformation step for any organization and a key area of interest for government to overcome these risks to physical medical records. The medical records processed and stored in digitized form on electronic media are called Electronic Health Records (EHR).

While EHR provides advantage over physical records, it faces its own set of security challenges with maintaining confidentiality, integrity, and availability of the data. The method of EHR data processing and storing follows the traditional server client model where centralized servers store and process the data and client front-end provides methods of retrieving it. The centralized servers can be a single point for vulnerability. Higher digitalization with less integration can lead to risk of data leakage, sniffing, cyberattacks and usually once hacker gains access, hacker encrypts the data to either blackmail of making the data public or not providing the decryption key unless ransom is paid. There are various healthcare IT standards currently used such as HIPAA law, Health level 7, and fast healthcare interoperability resources. Few other models used in healthcare systems are push, pull and view. Sharing this sensitive data among various entities through unsecure means can lead to leakage of the critical data. The critical issue in the EHR is maintaining the interoperability among various involved identities. These standards guide and, in some cases, mandate a series of controls to be implemented by the organization taking any part in handling of the medical records. Despite these guidelines, vulnerabilities continue to exist in these information systems impacting confidentiality, integrity, and availability of data.

1.1.1 Blockchain

Blockchain is a distributed ledger technology, which is used to record transactions in an unchangeable way. It has the ability to store information and data in blocks of information that cannot be altered once they have been recorded. This means that it can be trusted as there is no chance of any changes being made without permission from all parties involved. Blockchain also makes it possible for two or more parties to transact with each other without the need for a third party. The blockchain is a distributed database that maintains a continuously growing list of records. The information stored in the blockchain is not easily altered or tampered with and it is therefore considered immutable. Since this technology has been around for some time now, there are quite a few projects using it in various fields, including healthcare. Blockchain provides many advantages over traditional methods of storing patient data; these include transparency, security and accountability.

One of the key advantages of blockchain technology is its security. Because it is decentralized and distributed, it is not controlled by any single entity, making it resistant to tampering and fraud. In addition, the use of cryptographic techniques ensures that transactions are secure and can only be authorized by the parties involved.

Another advantage of blockchain is its transparency. All transactions on the blockchain are recorded and visible to all participants, allowing for increased accountability and trust. This can be particularly useful in industries where trust and transparency are important, such as supply chain management and the financial sector.

Furthermore, blockchain technology has the potential to improve efficiency and speed. Because it is a digital ledger, it can automate many of the processes that are currently done manually, such as the reconciliation of transactions. This can result in faster and more efficient transaction processing, with reduced costs and increased reliability.

Overall, blockchain technology offers many advantages, including improved security, transparency, and efficiency. These benefits have the potential to transform many industries, and we are likely to see continued adoption and development of blockchain technology in the coming years.

1.1.2 Medical records and their security

Critical patient data, for eras, has been maintained using paper copies and discs to include the crucial details of a patient’s health and wellbeing. The individuals working in this domain have always been extra cautions about handing this information as skillfully as possible. However, we’re only human and manual efforts from human beings are often prone to human error. In addition to this, this data is ideally expected to be maintained by authorized personnel working within the healthcare and research division only. However, due to the physical nature of data storage, one runs into the risk of this information getting into the wrong hands and being used for exploiting the healthcare organizations and their patients.

Storing records in a non-computerized format further runs into drawbacks such as extensive costs and accessibility issues. One needs to look after preserving the physical integrity of the documents from any type of mishandling. The cost involved in stationary supplies and printing and managing multiple copies of this data is quite extensive as well. However, the worst of all is the unfortunate losing of critical test information and having to request the patient to re-do the test that may have adverse effects on their medical conditions. Losing such information also makes the documentation incomplete, less accurate and reliable. Also, with the information only being available physically at a given location, it can only be accessed by specific individuals at any given time. Updating such information can be challenging and inaccurate to maintain across different sources.

Additionally, with the physical maintenance and duplication of data that is critical in nature, fragmentation between different healthcare providers causes the integrity of the patient data to be compromised. Medical institutions often struggle with maintaining longitudinal patient data due to nearly no exchange of data between different organizations. Each organization maintains their own version of the patient information based on their interaction with the patient and the patient records available to them from different sources. Due to this extensive fragmentation of information, it is a massive challenge to establish a central source of truth pertaining to the patients’ critical records.

To address the flaws within the traditional data storage model, electronic health record management systems have been proposed and implemented by organizations across the world. Integrating blockchain within these systems allows a level of security to be achieved. It provides a secure distributive database where all the queries run on the database are secure.

1.2 Motivation

Having considered the flaws associated with the traditional data storage methodologies, organizations migrated from paper-based system to an electronic records management may sound like a big step towards advancement and digitalization. However, not having the appropriate security measures integrated within the depths of this management system would only make this critical data be more susceptible to attackers and hackers. One such recent examples is the Cyber Attack on HSE in Ireland that took four months to bounce back fully from the attack. In May 2021, a ransomware cyberattack caused all the IT systems nationwide to shut down causing the staff to revert to using the paper based approach for maintaining patient information. The attackers encrypted 80% of the IT environment and prevented access to medical records and diagnostics thus causing a major outage throughout the country. The attackers got access to an extensive range of patient data from all age groups receiving their vaccinations due to the ongoing pandemic. This data was then exploited by the attackers to carry out Smishing, Vishing and Phishing attacks to acquire ransom and monetary gains.

1.3 Research Question

Can integrating blockchain improve the integrity and performance of the systems?
How Blockchain can be used to secure EHRs?
What are the challenges and important principles in blockchain while implementing EHRs based on it?

2 Related Work

In recent years, there has been growing interest in using blockchain technology to improve the security, transparency, and efficiency of EHR systems. Blockchain is a decentralized, distributed ledger technology that allows for the secure and transparent tracking of transactions. By leveraging the unique capabilities of blockchain, EHR systems can provide a secure and tamper-proof record of patient health information, while also ensuring privacy and interoperability.

There have been several studies and initiatives exploring the use of blockchain in EHR systems. For example, the American Medical Association has published guidelines for the use of blockchain in healthcare, highlighting the potential benefits and challenges of this technology. In addition, there have been several pilot projects and case studies that have demonstrated the feasibility and potential impact of using blockchain in EHR systems.

Overall, the use of blockchain in EHR systems has the potential to transform the way that health information is managed and shared, and is an area of active research and development. This study aims to contribute to the existing body of knowledge on this topic by providing an in-depth examination of the potential benefits and challenges of using blockchain in EHR systems.

2.1 Current state-of-art in securing HER

(Kruse *et al.*, 2017) talk about modern technology advancements and how healthcare organizations are targeted for security breaches. The group used security and EHR as the search criteria and analysed different security techniques for EHR by reviewing 25 papers out of 2451 papers from 3 different databases. Three categories of safeguards were used to analyse the papers: Administrative, Physical and Technical. The most common security technique which was determined was the implementation of firewalls to protect the EHR systems and states that technical security measures may not be sufficient as the version of ransomware/viruses keep modifying. Using 25 papers 40 safeguards techniques were identified out of which 45% were Technical, 17.5% Administrative, 12.5% Physical and 25% others. The limitation of this paper is that it does not identify which safeguard methods are comparatively better or lesser than the other candidates of this study. It only provides a survey of security and safeguard techniques, their categories, and their categorisations.

(Sahi, Lai and Li, 2021) explain the high demand of security and privacy requirements to store health records on cloud. The advantages and drawbacks of data encryption are discussed in a thorough assessment encompassing 132 studies from numerous peer-reviewed databases, including IEEE Xplore. Additionally, this study contrasts a number of studies in the field of data security needs. Numerous unresolved issues are discussed along with outdated systems being used which are prone to cyberattacks and require high amount of maintenance to keep them secure. They point out 12 data security requirements and create a comparison of security approaches.

(Sahi *et al.*, 2018) provide an overview of the current e-Healthcare system architecture and the security issues faced. The authors point out that the present e-Healthcare platforms are not yet fully developed and mature, they lack the level of user data security, secrecy, and integrity that is required for widespread adoption. One of the largest challenges to e-healthcare systems' effectiveness in gaining patients' trust is privacy. A thorough review of privacy preservation techniques is carried out along with suggestions to overcome privacy challenges such as use of data anonymization, patient centric access control and propose a two-tiered access control in the healthcare systems. This article reviews previous studies in this field and proposes a high-level outline of a privacy-preserving method that takes into account all pressing privacy issues.

2.2 Blockchain implementations

(Golosova and Romanovs, 2018) studied numerous blockchain applications that have already been put into use as well as aspects that affected deployment and the challenges faced during implementation of the current systems. The authors examine the benefits and challenges of integrating and applying blockchain technology across many current industrial sectors. The use of blockchain resolved a few issues with the centralized system, including the transaction time and the accidental or deliberate deletion or change of data. All the attacks that are mentioned are either theoretical or can disrupt the work on the system but not technology. The implementation of blockchain technology can aid in resolving a variety of complex issues that are obstructing and impairing how systems operate properly. Although using the Blockchain has many hurdles, the benefits outweigh the drawbacks by a wide margin.

(van der Heijden *et al.*, 2017) propose a event data recorder based on blockchain for security in vehicle-to-x communication. The idea is to develop a distributed event data recorder (EDR) that satisfies traditional accountability criteria. The proposed distributed ledger solution, in contrast to other methods, offers an accountable revocation method by enabling a collaborative and open decision-making mechanism. Blackchain combines a distributed ledger with already-existing security mechanisms in V2X communication systems. Individual vehicles dynamically form clusters, which then submit their consensus decisions as input to road-side units (RSUs), which in turn report their findings to disciplinary authorities.

(Tijan *et al.,* 2019) provide a thorough analysis of the prevailing and emerging trends in the application of blockchain technology in logistics and supply chain management. Although the banking industry has received the most attention on the advantages of blockchain technology, the authors point out significant logistical difficulties that can be reduced by using blockchain technology, notably order delays, inaccuracies, and multiple data entry. The research is limited to understanding the benefits and challenges of implementation and does not propose a solution.

(Udokwu *et al.*, 2018) list the characteristics of smart-contract applications in many contemporary organization sectors and further examine and identify issues that hinder the implementation of smart-contract apps. The use of smart contracts in enterprise apps may be constrained by the cost associated with completing transactions on the blockchain in order to pay miners. However, as permissioned blockchains typically use voting-based consensus techniques, this does not apply to private blockchain networks. 87.5% of the firms using smart-contract applications are private. 75 percent of currently active initiatives are made particularly for private businesses. A few of the main benefits of implementing smart contracts are transparency and trust.

(Gimenez-Aguilar *et al.*, 2021) provide a comprehensive review of techniques that have been proposed or implemented to achieve cyber security in blockchain based systems. The authors also study the trends of the security techniques from year 2013 to 2020 and provide comparative data based on the industry the techniques are more used in.

2.3 Using Blockchain in EHR

(Sharma *et al.*, 2022) review the security of current EHR systems and propose a blockchain based data management for healthcare systems. The study is focused on 6 issues in order to achieve 4 objectives which are Secure data storing, sharing, audit and authentication. The study also provides a comparison of proposals and solutions made in healthcare based on blockchain.

(Azaria *et al.*, 2016) create a working prototype of Medical data access and permission management based on blockchain which caters to the problem of security as well as data management across different organizations keeping the users' interests at the centre of it. The research does not address the challenge of migrating from the current healthcare systems to the Blockchain based design.

(Rajadevi *et al.*, 2022) propose and implement a secured storing and sharing of medical records on blockchain. The main benefits of the proposed design helps with data integrity. The paper explains the maintenance and sharing of electronic information through blockchain. It is limited to implementation of 1st part of the proposal and no data analysis or evaluation is done.

(Mahdy, 2021) propose a distributed system to enable secure sharing of health records based on semi centralized blockchain. The paper focuses on high data reproducibility and availability. The proposed design uses end to end encryption using RSA key pair. Software solution is not implemented for proposed design.

3 Research Methodology

The first step starts with modelling a EHR system, study the current issues & vulnerabilities and to study the use of blockchain in these systems. The approach for this research will be a mixed method approach. For development of the project, Secure SDLC methodology waterfall model was chosen. Evaluation will be carried out in multiple phases.

3.1 SDLC & Secure SDLC

Software development life cycle (SDLC) is a framework that describes the steps involved in developing a software application. (Velimirovic, 2022) It typically includes the following stages: planning, analysis, design, implementation, testing, deployment, and maintenance. The goal of the SDLC is to create a high-quality software product that meets the needs of the user. The first step in creating an application involves gathering and analyzing requirements to determine the goals and scope of the project. This phase is important for planning and identifying the necessary resources, time duration, cost, risks, benefits, and other aspects involved in building the application. It is also crucial for analyzing customer needs and determining the resources required to build the application. The next step is design, where the architecture, user interface, communication, platforms, security features, and other documentation are described. After design, developers write code in a chosen programming language according to coding guidelines. The application is then tested to ensure it is working as required. This step helps to identify and fix defects or bugs, leading to better performance. Once testing is complete, the application is deployed in a real environment for actual use. Finally, maintenance is performed to fix any remaining bugs, add new features, and upgrade the application as needed.

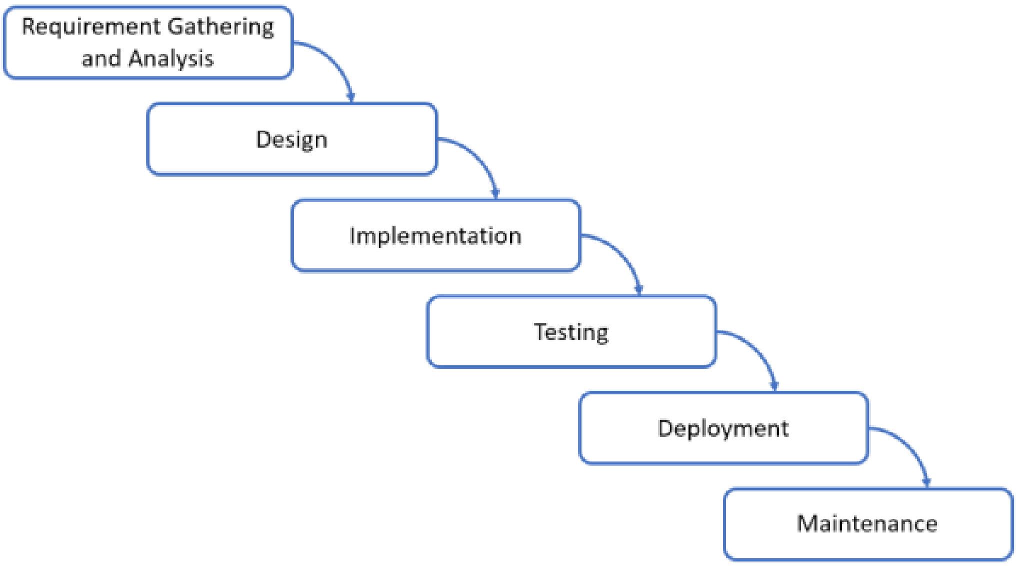


Fig 3.1.1: SDLC

One important aspect of the SDLC is security. In a secure SDLC, security is considered throughout the entire development process, rather than as an afterthought. This involves incorporating security measures into each stage of the SDLC(*The Secure Software Development Lifecycle Explained*), from the initial planning and analysis stages, to the final deployment and maintenance stages.

For example, during the planning stage, a secure SDLC would include activities such as identifying potential security risks and vulnerabilities, and developing a plan to mitigate those risks. During the design stage, a secure SDLC would involve incorporating security measures such as encryption, authentication, and access controls into the software design.

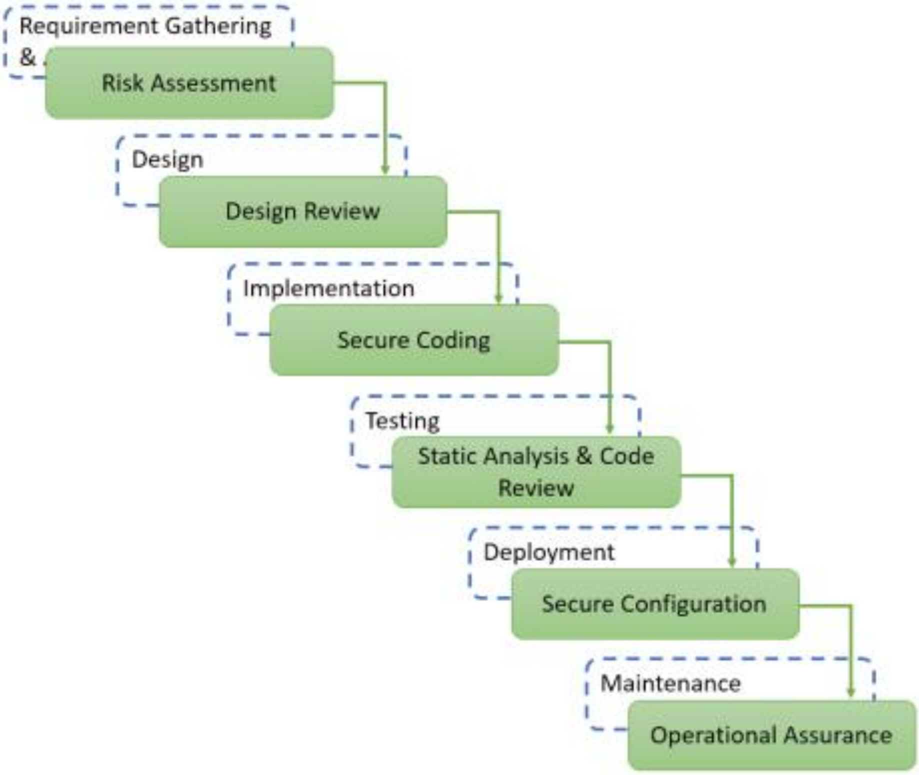


Fig 3.1.2: SSDLC

During the implementation stage, a secure SDLC would involve testing the software for security vulnerabilities and ensuring that it meets security standards and requirements. This could involve conducting penetration testing, security audits, and other types of testing to identify and address any potential security issues.

In the testing stage, a secure SDLC would involve conducting thorough testing of the software to ensure that it functions properly and meets the user's needs. This could include testing the software's security features, as well as its overall functionality and usability.

Finally, in the deployment and maintenance stages, a secure SDLC would involve ongoing monitoring and maintenance of the software to ensure that it continues to function properly and remains secure. This could involve regular security updates and patches, as well as monitoring for potential security breaches or vulnerabilities.

Overall, a secure SDLC is essential for ensuring that software applications are secure and meet the needs of the user. By incorporating security measures into each stage of the SDLC, developers can create high-quality software that is secure and reliable.

3.2 Blockchain Vulnerability Scoring System (BVSS)

A blockchain vulnerability scoring system is a system that uses a set of criteria and metrics to assess the security and vulnerability of a blockchain network.

The scoring system is typically based on a set of parameters such as the type of consensus mechanism used, the number of nodes on the network, the level of decentralization, the number and severity of past vulnerabilities, and the frequency of security updates.

Based on these parameters, the scoring system assigns a vulnerability score to the blockchain, which can be used to evaluate its overall security and vulnerability.

The use of a blockchain vulnerability scoring system allows for a more transparent and objective assessment of the security of a blockchain network, enabling users and stakeholders to make informed decisions about their use and adoption of the technology.

4 Design Specification

4.1 Architecture

Traditional electronic hospital records were maintained in a centralized database usually on premise or it could be on cloud. The general idea was the records will be stored in one location and requisite people will have access to it. It has been observed that traditional databases have certain limitations and one of the biggest one in terms of security is integrity, if you look at it in terms of CIA triad the biggest is integrity. All the users on the EHR are registered through the public blockchain id. Accounts have role based access control. The first account is activated as the admin and has limited access to personal data. Users connect to the EHR system using their Ethereum account and every request or booking or prescription is recorded as a new transaction in the blocks. Smart contracts are deployed by the admin. Healthcare providers, technicians and insurance companies have to request data from the patient to access. Patient can grant and deny access of their data to anyone. Any changes to a block is recorded as a new block with the last block attached making it impossible to tamper with data. Use case designs is done based on the 3 users Admin, Patient and Doctor. This is access based control using smart contracts. The smart contracts are instances of contracts deployed on the Ethereum blockchain.

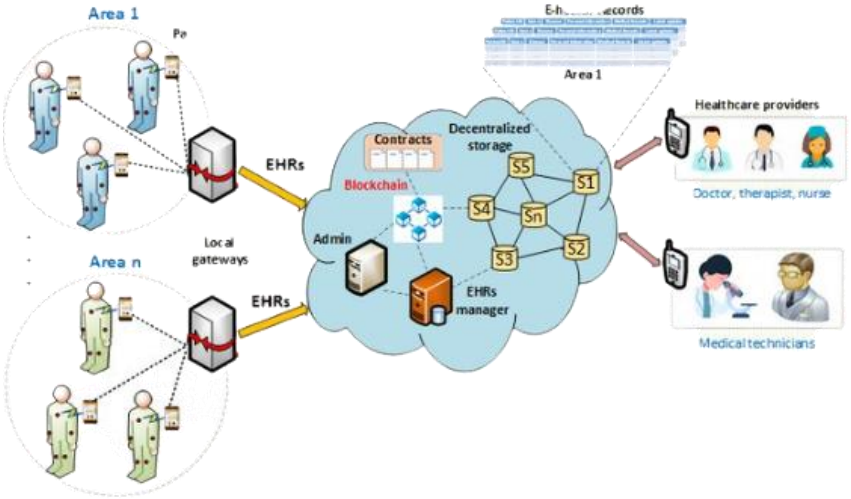


Fig 4.1.1: Basic architecture

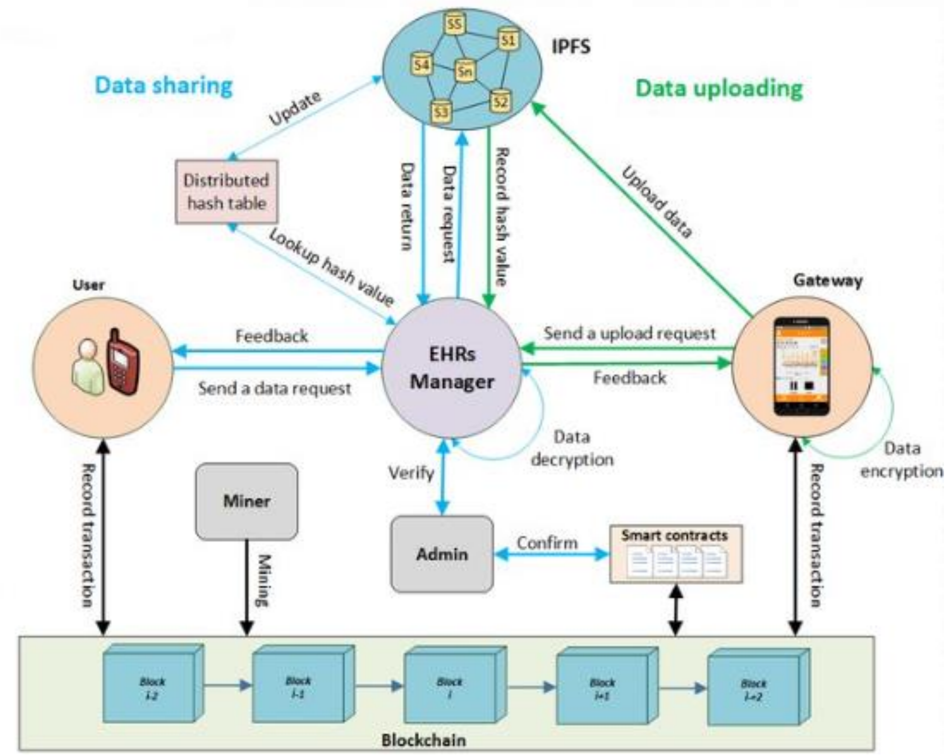


Fig 4.1.2: Data flow (Sharing & Uploading)

4.2 Users Use Case

Patient Use Case

Patient should have good control over their personal data. Patient can view all self-details, edit personal details, view list of all doctors, grant or revoke data access to a doctor and view history of own personal data.

Doctor Use Case

Doctor can view self-details, view current medical details, list of patients that can be accessed by the doctor or list of patients who have granted access to their data which can be used to view current medical details of them, edit details base on reports and view history of the patient.

Admin Use Case

Admin can create patient with personal and medical details, create doctor account in its own hospital and view list of patients with limited amount of data. So that not everything is accessible to them.

4.3 Ethereum

The Ethereum blockchain is a decentralized, open-source platform that allows for the creation and execution of smart contracts. These are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This makes it possible for transactions to be carried out automatically and trustlessly, without the need for a third party intermediary.

In the context of an EHR system, the Ethereum blockchain could potentially be used to securely store and manage patient health records. This could be done through the use of smart contracts to automate the management of access to the records, ensuring that only authorized individuals are able to view or modify the information. Additionally, the use of the blockchain could provide a tamper-evident record of all changes made to a patient's health records, allowing for greater transparency and accountability in the handling of sensitive medical information. The Ethereum blockchain could be utilized for electronic health records (EHR) in several ways:

Secure and decentralized storage: The blockchain provides a secure and decentralized platform for storing EHR data, allowing for easy access and secure sharing of information among healthcare providers and patients.

Audit trail and data integrity: The transparent and immutable nature of the blockchain allows for a clear audit trail of all EHR data, ensuring data integrity and preventing tampering or unauthorized access.

Streamlined data sharing: The use of smart contracts on the Ethereum blockchain could enable automated and streamlined data sharing among healthcare providers, reducing the need for manual data entry and improving data accuracy.

Patient control: Patients could have complete control over their own EHR data and grant access to healthcare providers on their own terms, empowering them to take charge of their health and privacy.

Overall, the use of the Ethereum blockchain for EHR has the potential to improve data security, accessibility, and accuracy, ultimately leading to better healthcare outcomes.

4.4 Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They are executed and enforced by the blockchain network, allowing for the automation of complex processes without the need for intermediaries. Some key features of smart contracts include:

- Autonomy: Smart contracts are self-executing and do not require manual intervention to be carried out.
- Trust: The decentralized and transparent nature of the blockchain ensures that the terms of the contract are transparent and cannot be altered once deployed.
- Efficiency: Smart contracts can automate complex processes, reducing the need for manual intervention and speeding up transactions.
- Security: The use of cryptography ensures that smart contracts are secure and cannot be tampered with.

Overall, smart contracts offer a powerful tool for automating and streamlining complex processes, reducing the need for intermediaries and improving trust and efficiency.

The Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) are two important regulations that pertain to the handling and protection of personal health and data. Smart contracts can be utilized to ensure compliance with both HIPAA and GDPR in several ways:

- Secure and decentralized storage: The blockchain provides a secure and decentralized platform for storing personal health and data, allowing for easy access and secure sharing of information while ensuring compliance with HIPAA and GDPR.
- Audit trail and data integrity: The transparent and immutable nature of the blockchain allows for a clear audit trail of all data, ensuring data integrity and preventing tampering or unauthorized access, which is crucial for compliance with HIPAA and GDPR.
- Patient control: Smart contracts can enable patients to have complete control over their own health and data, and grant access to healthcare providers on their own terms,

empowering them to take charge of their health and privacy, which is a key requirement of both HIPAA and GDPR.

Overall, the use of smart contracts for HIPAA and GDPR compliance can improve data security, accessibility, and accuracy, ultimately leading to better healthcare outcomes while ensuring compliance with important regulations.

The registry contract is used to register all users on the blockchain in an anonymous manner. This protects the system from malicious users who may try to add fake data or misuse data. The registry contract stores each user's public key and their role (e.g. patient, care provider, researcher, regulator) and miners check the legitimacy of users when validating transactions sent to the data contract and permission contract. The data contract stores a list of records that indicate the mapping between users and their data, including the public key of the data owner, the symmetric key encrypted using the public key, the type of data, and the hash of the data. The permission contract keeps a record of access permissions for different users, indicating their privileges on data that resides in the data contract. The permission contract allows for the requesting, granting, and modifying of permissions.

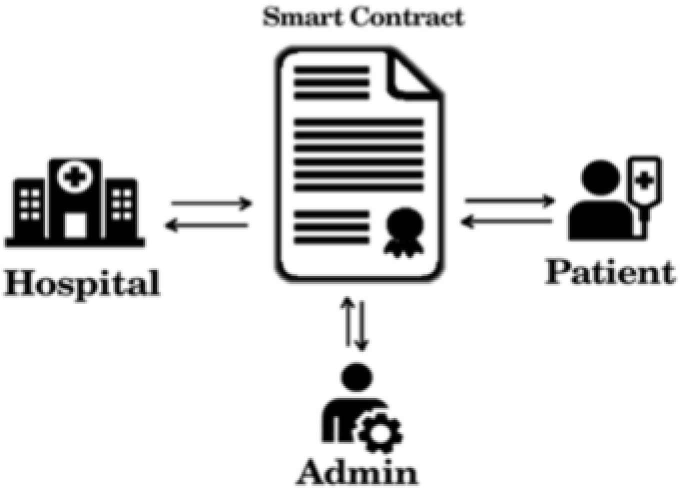


Fig 4.4.1: Smart Contracts

The proposed smart contract framework for electronic health records (EHR) is a system that utilizes the Ethereum blockchain to enable hospitals and healthcare institutions to securely share and manage patient records. The administrator is responsible for registering healthcare institutions on the application and has the ability to create, edit, add, and suspend hospital accounts. When a new patient record is created, a new block is created, verified, and broadcasted to all nodes on the network, and added to the blockchain. Hospitals can request access to a patient's records and schedule appointments, but the patient has the ability to grant or deny access to their records. This design ensures data exchange is streamlined and data security and privacy are maintained through the use of blockchain technology.

5 Implementation

EHR model based on Ethereum blockchain is implemented/developed using multiple languages in VScode IDE. The tools and languages used to produce the output are:

5.1 Ganache/Truffle suite

Ganache is a local blockchain network that was used for Ethereum development. It provides a quick and easy way to create a private blockchain and test smart contracts without the need for a live network. The Truffle Suite is a set of tools that are used for Ethereum development, including Truffle, a development framework for writing and deploying smart contracts, and Ganache, a local blockchain network for testing and debugging. Together, the Ganache and Truffle Suite provide developers with a comprehensive set of tools for developing and testing Ethereum applications and smart contracts. They were used in the development process to create and deploy contracts, test them, and debug any issues before deploying to a live network.

5.2 Metamask – Blockchain client

It is a web browser extension that allows users to interact with the Ethereum blockchain. It acts as a wallet, enabling users to manage their Ether (ETH) and other Ethereum-based assets, as well as interact with decentralized applications (dApps) on the Ethereum network. It provides an easy-to-use interface for users to manage their blockchain accounts and transactions, making it accessible to even those who are new to the world of blockchain and cryptocurrency.

It also allows users to switch between different Ethereum networks, such as the main network, test networks, and private networks. Overall, MetaMask is a popular and user-friendly tool for accessing and interacting with the Ethereum blockchain. It enables users to easily manage their Ethereum-based assets and interact with dApps, making it an essential part of the Ethereum ecosystem.

5.3 Javascript & Typescript - Backend

JavaScript is a high-level, interpreted programming language that is commonly used to add interactivity and dynamic behavior to websites. It is a prototype-based, object-oriented language that supports event-driven, functional, and imperative programming styles. JavaScript was used to create client-side scripts that run in web browsers, as well as by server-side developers to create server-side scripts that run on web servers. JavaScript is supported by all major web browsers, and it is typically used alongside HTML and CSS to create dynamic and interactive web applications. TypeScript is a typed superset of JavaScript that compiles to plain JavaScript. It adds optional static typing and class-based object-oriented programming to the language. It is designed to improve the development experience by catching errors before they occur at runtime, making it easier to write and maintain large, complex codebases. TypeScript is widely used in the development of large-scale JavaScript applications, and it is supported by popular development tools such as Visual Studio, WebStorm, and Eclipse.

5.4 HTML & CSS - Frontend

HTML (HyperText Markup Language) and CSS (Cascading Style Sheets) were two technologies that were used together to create the structure and style of a web page. HTML is a markup language that is used to define the content and structure of a web page, while CSS is a stylesheet language that is used to add styling, such as colors, fonts, and layout, to the content of a web page. Together, HTML and CSS are the building blocks of the web, and they are essential technologies for any web developer to learn. HTML and CSS are both simple languages that are easy to learn and use, but they are also powerful tools that can be used to create complex, dynamic, and interactive web applications.

5.5 Solidity - Backend

Solidity is a high-level, contract-oriented programming language used for writing smart contracts that were run on the Ethereum blockchain. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Solidity was used to write these smart contracts, which are then compiled and deployed to the Ethereum blockchain. Once deployed, the smart contract can be executed automatically, without the need for third-party intermediaries. Solidity is a relatively new language, but it is quickly gaining popularity among blockchain developers, as it enables them to easily create and deploy smart contracts on the Ethereum blockchain.

5.6 Security Implementations

-RBAC (Role based access control)
-Authentication and authorization
-Data encryption

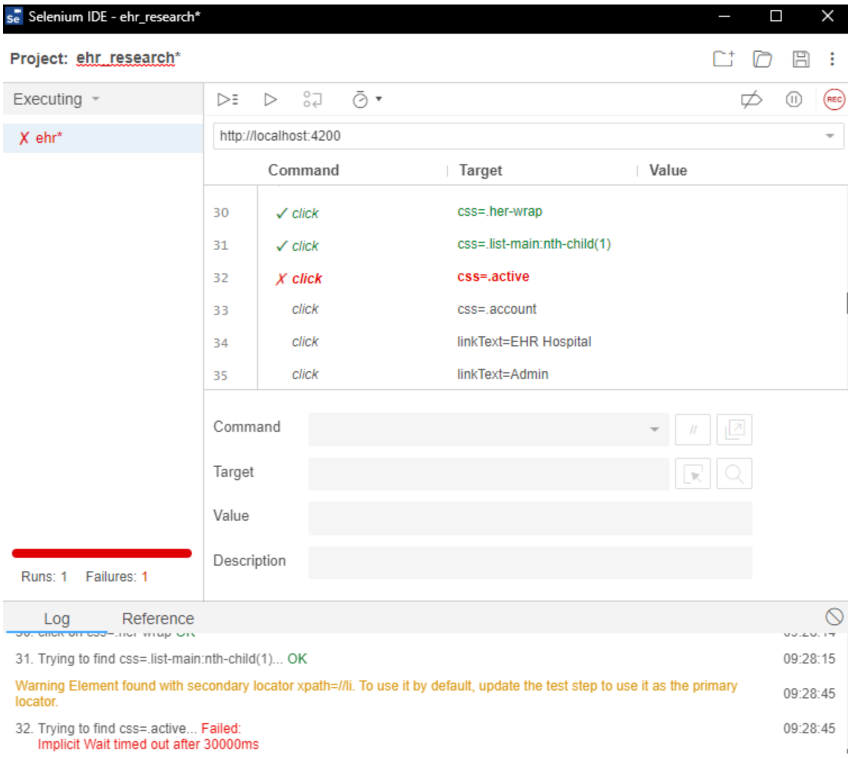
5.7 Yarn

Yarn package is used to manage the dependencies of the project, such as libraries and frameworks. Yarn is used to run the script.

6 Evaluation

6.1 Functional Evaluation – Selenium IDE

Selenium IDE is a tool for recording and playing back user interactions with a web application in order to automate functional testing. It allows you to create and run automated tests for your web application in the browser, without the need to write any code. This can be useful for catching bugs and ensuring that your application is working properly.



	Command	Target	Value
30	✓ click	css=.her-wrap	
31	✓ click	css=.list-main:nth-child(1)	
32	✗ click	css=.active	
33	click	css=.account	
34	click	linkText=EHR Hospital	
35	click	linkText=Admin	

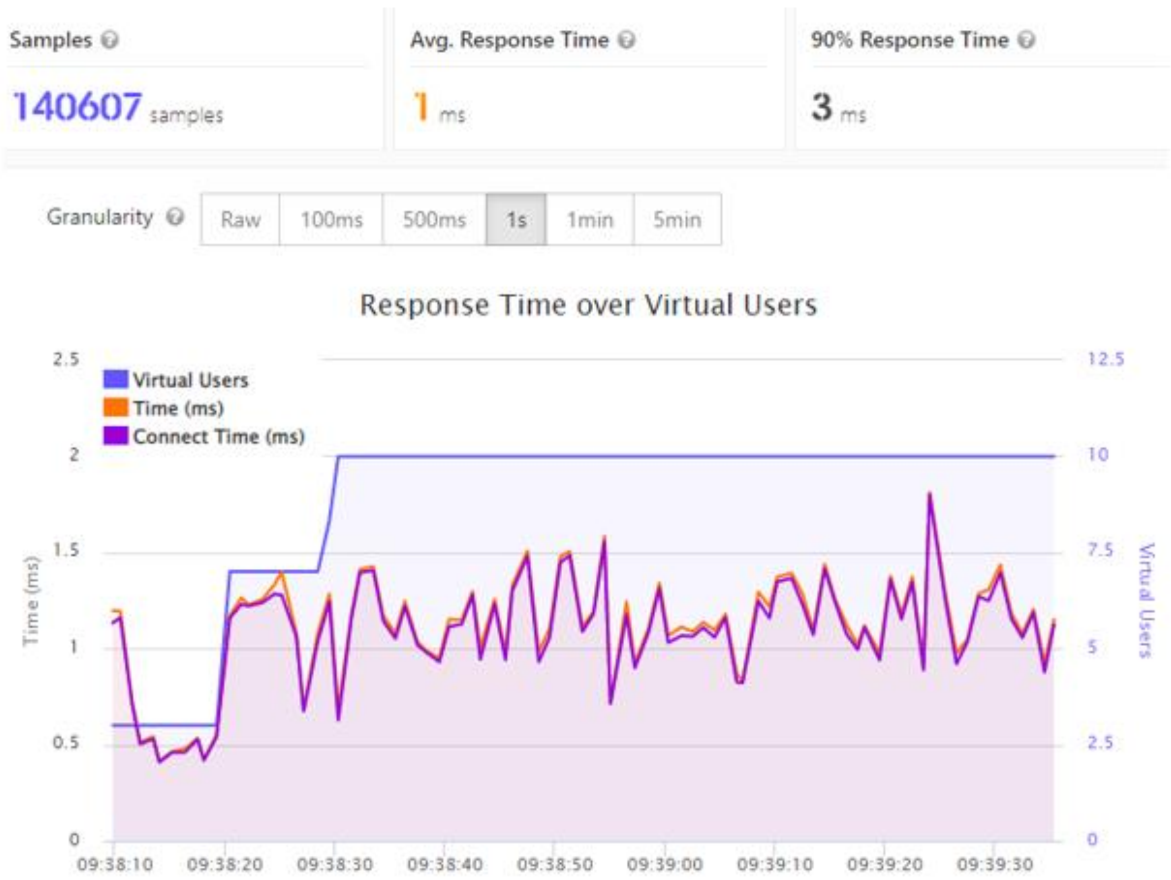
```
31. Trying to find css=.list-main:nth-child(1)... OK                                            09:28:15
Warning Element found with secondary locator xpath=//li. To use it by default, update the test step to use it as the primary
locator.                                                                                         09:28:45
32. Trying to find css=.active... Failed:                                                        09:28:45
    Implicit Wait timed out after 30000ms
```

Fig 6.1.1: Selenium Functional testing

Functional testing of application involves testing each functional area of the application.

6.2 Operational/Performance Evaluation – LoadFocus

Performance testing is essentially testing of application under measured load and identifying how well the application can handle it. Some parameters that are controlled during performance testing are a set number of users accessing the application and its features within a small frame of time. For this project, the testing application used is LoadFocus which performs automated load tests on a web application through virtual users. The choice of LoadFocus was made as it is a cloud-based online platform and does not require any installation. It also has most features available on the free tier. One drawback on the free tier is the report is not available for download, but screenshots of the report are attached in this section. For this test, LoadFocus deployed 10 virtual users over a period of 60 seconds. About 140607 samples were collected and results shows an average response time of around 1 millisecond for user input. The site was hosted locally for this test.



Samples 140607 samples

Avg. Response Time 1 ms

90% Response Time 3 ms

Granularity: Raw | 100ms | 500ms | **1s** | 1min | 5min

Fig 6.2.1: Loadfocus load testing

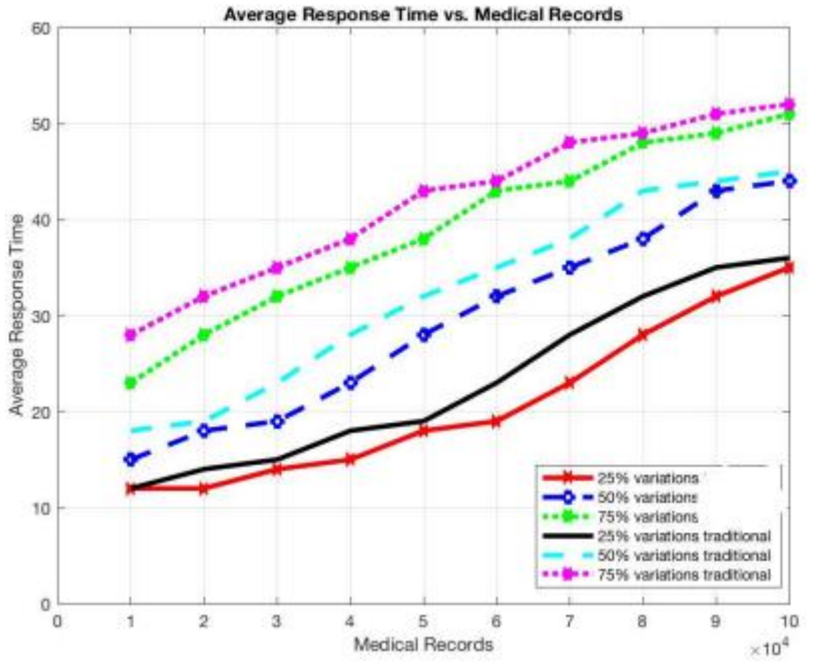
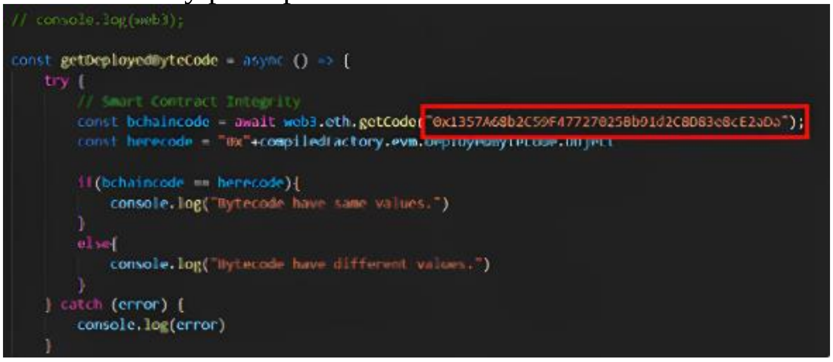


Fig 6.2.2: Avg respone time(EHR blockchain vs traditional relational database) Loadfocus Jmeter

6.3 Security Evaluation

6.3.1 Data integrity

To determine if the smart contract data stored on the Ethereum network will be safe from changes made by third parties during deployment, the integrity test is carried out. The first step is to compile the smart contract. The next step is to enter the address of the deployed contract into the private blockchain network. If the bytecode of the executed file is the same, it can be confirmed that the contract's data has not been altered. The output of this process is shown in Figure. If the integrity test is successful, it can be concluded that the system meets the integrity requirement of the CI security principles.

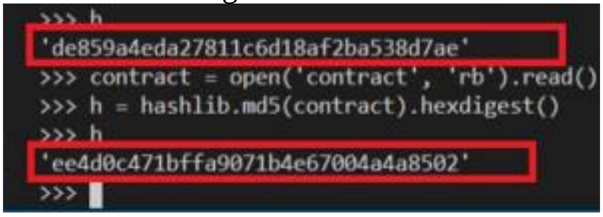


```
// console.log(web3);

const getDeployedBytecode = async () => {
    try {
        // Smart Contract Integrity
        const bchaincode = await web3.eth.getCode("0x1357A68b2C59F47727025Bb91d2C8D83e8cE2aDa");
        const herecode = "0x"+compiledFactory.evm.deployedBytecode.object

        if(bchaincode == herecode){
            console.log("Bytecode have same values.")
        }
        else{
            console.log("Bytecode have different values.")
        }
    } catch (error) {
        console.log(error)
    }
```

Fig 6.3.1: Same Bytecode Determined

6.3.2 Hash test

Checking if changing a letter in the contract changes the hash of the block or not. Using python hashlib in command prompt. Changing a letter does change the hash value and after undoing the changes the hash value changes to the first one.



```
>>> h
'de859a4eda27811c6d18af2ba538d7ae'
>>> contract = open('contract', 'rb').read()
>>> h = hashlib.md5(contract).hexdigest()
>>> h
'ee4d0c471bffa9071b4e67004a4a8502'
>>> 
```

Fig 6.3.2: Changing a letter changes the hash value

6.4 Discussion

This research aims to provide a better solution for storing and managing data for patients in Ireland. The goal is to keep the data safe and secure, with each patient having a unique identifier. The study used various techniques and methods to develop a user-friendly technology application. The first experiment tests the functionality of the dApp followed by a performance load test. Another experiment with the Python library Hashlib tested the logic of the library and provided a clear approach for testing and seeing results. Challenges for the project included the learning curve for blockchain technology and investment in new solutions. Future work could involve integrating the applications and expanding the concept to other areas of healthcare. Overall, the tests and results were favourable and suggest that this strategy could have a positive impact on data handling for patients in Ireland.

7 Conclusion and Future Work

Electronic health records (EHRs) are digital versions of patients' medical histories. While EHRs have addressed many challenges related to data transfer and storage, there are still unresolved issues associated with their implementation. A thorough study is necessary to identify potential errors and develop solutions to minimize these issues. Previous research has shown that EHR implementation is fraught with challenges, including data management and privacy concerns. Along with time electronic health record (EHR) systems need to be regularly updated and also upgraded in order to maintain their accuracy and effectiveness. As medical knowledge and technology advance, EHR systems need to be updated with new information and features in order to provide the most up-to-date and relevant care for patients. In addition, EHR systems must be regularly maintained and upgraded in order to protect against security threats and ensure the privacy and security of patients' personal and medical information. Regular updates are crucial for the successful operation and continued improvement of EHR systems. The proposed model shows positive results in terms of data confidentiality, integrity and performance of the decentralised application.

Future work could include implementation on bigger scale or even seamless transition from current traditional relational database based EHRs to blockchain based EHRs. Future work could also include implementation of a Blockchain vulnerability scoring system integrated into the system to evaluate the security of the system. BVSS would help in assessing the security of individual functions that are being implemented in real-time. Semi-centralized blockchain are also growing and have been proving really affective in terms of private sharing and can even improve the proposed model in terms of private governance.

References

Azaria, A. *et al.* (2016) ‘MedRec: Using Blockchain for Medical Data Access and Permission Management’, in *2016 2nd International Conference on Open and Big Data (OBD). 2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25–30. Available at: https://doi.org/10.1109/OBD.2016.11.

Fatokun, T., Nag, A. and Sharma, S. (2021) ‘Towards a Blockchain Assisted Patient Owned System for Electronic Health Records’.

Gimenez-Aguilar, M. *et al.* (2021) ‘Achieving cybersecurity in blockchain-based systems: A survey’, *Future Generation Computer Systems*, 124, pp. 91–118. Available at: https://doi.org/10.1016/j.future.2021.05.007.

Golosova, J. and Romanovs, A. (2018) ‘The Advantages and Disadvantages of the Blockchain Technology’, in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pp. 1–6. Available at: https://doi.org/10.1109/AIEEE.2018.8592253.

van der Heijden, R.W. *et al.* (2017) ‘Blackchain: scalability for resource-constrained accountable vehicle-to-x communication’, in *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*. New York, NY, USA: Association for Computing Machinery (SERIAL ’17), pp. 1–5. Available at: https://doi.org/10.1145/3152824.3152828.

Kruse, C.S. *et al.* (2017) ‘Security Techniques for the Electronic Health Records’, *Journal of Medical Systems*, 41(8), p. 127. Available at: https://doi.org/10.1007/s10916-017-0778-4.

Mahdy, M.M. (2021) ‘Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records’, in *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE). 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, pp. 1–4. Available at: https://doi.org/10.1109/ICCCEEE49695.2021.9429554.

Rajadevi, R. *et al.* (2022) ‘Secured Storing and Sharing of Medical Records Based on Blockchain’, in *2022 International Conference on Computer Communication and Informatics (ICCCI). 2022 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–5. Available at: https://doi.org/10.1109/ICCCI54379.2022.9741070.

Sahi, A., Lai, D. and Li, Y. (2021) ‘A Review of the State of the Art in Privacy and Security in the eHealth Cloud’, *IEEE Access*, 9, pp. 104127–104141. Available at: https://doi.org/10.1109/ACCESS.2021.3098708.

Sahi, M.A. *et al.* (2018) ‘Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions’, *IEEE Access*, 6, pp. 464–478. Available at: https://doi.org/10.1109/ACCESS.2017.2767561.

Sharma, V. *et al.* (2022) ‘Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions’, *Security and Communication Networks*, 2022, p. e9697545. Available at: https://doi.org/10.1155/2022/9697545.

The Secure Software Development Lifecycle Explained (no date) *Digital Maelstrom*. Available at: https://www.digitalmaelstrom.net/it-security-services/secure-software-development-lifecycle-ssdlc/ (Accessed: 14 December 2022).

Tijan, E. *et al.* (2019) ‘Blockchain Technology Implementation in Logistics’, *Sustainability*, 11(4), p. 1185. Available at: https://doi.org/10.3390/su11041185.

Udokwu, C. *et al.* (2018) ‘The State of the Art for Blockchain-Enabled Smart-Contract Applications in the Organization’, in *2018 Ivannikov Ispras Open Conference (ISPRAS). 2018 Ivannikov Ispras Open Conference (ISPRAS)*, pp. 137–144. Available at: https://doi.org/10.1109/ISPRAS.2018.00029.

Velimirovic, A. (2022) *What is SDLC? Understand the Software Development Life Cycle*, *phoenixNAP Blog*. Available at: https://phoenixnap.com/blog/software-development-life-cycle (Accessed: 14 December 2022).