JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PBFT-Driven Blockchain Framework for the Security of Electronic Health Records

Mrs. Deepa Patel, Mr. Rajneesh Pachouri, Mr. Anurag Jain, Mrs. Monali Sahoo

Research Scholar, Assistant Professor, Department of Computer Science & Engineering

Adina Institute of Science & Technology, Sagar India.

Abstract : Because Cloud Health Record (CHR) has documented the onset, progression, and management of illnesses, it is extremely valuable from a medical standpoint. Given the sensitive and private nature of patient medical data, cloud health records (CHR) are vital and personal documents for each and every patient. Privacy preservation, security, and data exchange are important CHR concerns. Improved security and user experiences are just two of the numerous advantages that come with technological innovation, and these have been crucial to the popularity of cloud health records in recent years. Nonetheless, there are still a lot of problems with users' complete ownership of data integrity and the security of medical records. Blockchain technology is a novel approach that may be suitable for addressing the difficulties that have been highlighted. Medical records and other healthcare-related data can be housed on a well-architected, secure, tamper-proof platform thanks to technology. To protect privacy, cryptographic procedures are used. The model has tamper resistance, auditability, revocability of consent, and fine-grained and flexible access control. A thorough examination of security would demonstrate that the approach is provably safe in terms of tamper resistance and privacy. The results of the performance analysis indicate that the model outperforms the current approach used in the literature review in terms of overall performance.

IndexTerms **- Cloud Health Record, Blockchain technology, Cryptographic, performance analysis, flexible access control.**

I. INTRODUCTION

Background Study Of Study

Prior to the development of contemporary technology, the healthcare industry kept medical records on paper using a handwritten method. This medical record system, which was based on paper, was unreliable, unsafe, disorganised, and not resistant to agitation. Due to the fact that the patient's medical records were duplicated and redundant in all of the institutions they visited, it too had to deal with this problem.

Problem Statement

Some of the factors that contributed to the creation of this system are listed below: Asymmetry of Information: Healthcare practitioners and patients frequently transmit inconsistent information about medical errors, patient dissatisfaction, and over- and under-treatment, with the majority of them occurring in the poor world and the western world. Ensuring equal information interchange will guarantee patient engagement, improved outcomes, and a decrease in needless medical expenses.

Data Breaches:

Breach in the healthcare industry has long been a problem, according to the US Department of Health and Human Services Office for Civil Rights. More than 3,054 healthcare data breaches involving more than 500 records have occurred between 2009 and 2019. More than 230,954,151 medical records have been lost, stolen, exposed, or improperly disclosed as a result of such breaches. That is equivalent to more than 69.78% of the US population.

The frequency and extent of electronic health care data breaches are expected to rise in light of the rapid expansion of Cloud Health Record deployment since 2012 and the anticipated rise in cloud-based services offered by vendors supporting predictive analytics, personal health records, health-related sensors, and gene sequencing technology.

Project Motivation

The use of Cloud Health Records (CHR) is spreading throughout many developing nations. It is crucial because it raises the standard of healthcare. There is uncertainty about this technology due to recent reports of security breaches. The potential ethical problems are not receiving much attention, despite its growing use and the fervour with which it is being adopted. This idea was inspired by how frequently healthcare data breaches occur.

The goal of this project is to apply a blockchain-based Cloud Health Record/medical record for security, integrity, privacy, information asymmetry, and data interoperability in order to enhance and expand on previous work.

Project Objectives

The objectives of this project is to develop a blockchain-based Cloud Health Record system that;

- Protects the privacy, confidentiality, and integrity of Cloud Health Records.
- Addresses data interoperability, which is the unsafe exchange of patient medical records across healthcare facilities.
- Addresses the problem of information asymmetry, giving patients improved access to their medical records

- ❖ Implementation of 'a', 'b' and 'c' above.

Contribution To Knowledge

It is expected that the proposed work would do the following;

- ❖ Solve information asymmetry and data interoperability problems between healthcare providers and institutions.
- ❖ Secure cloud health records and patient medical records effectively, offering integrity, privacy, and secrecy by keeping the health records in a blockchain.

Possible Challenges

Acquiring a comprehensive understanding of blockchain technology and its application The amount of time needed to finish the work.

The recent advancement of technology is having an impact on every aspect of human existence and altering how we utilise and view the world. Similar to the improvements technology has brought about in other spheres of life, it is likewise discovering new avenues for advancement in the healthcare industry. The enhancement of security, user experience, and other aspects of the healthcare sector are the primary advantages that come with technological advancements. Electronic Medical Record (EMR) and Electronic Health Record (EHR) systems provided these advantages. They still have some problems, though, with data integrity, user ownership, and security of medical records, among other things. One potential answer to these problems could be the application of a new technology called Blockchain. With the use of this technology, medical records and other data pertaining to healthcare can be stored on a safe, temperature-resistant platform. Prior to the development of contemporary technology, the healthcare industry kept medical records on paper using a handwritten method.

This medical record system, which was based on paper, was unreliable, unsafe, disorganised, and not resistant to agitation. Due of several copies of the patient's medical records at each institution they visited, it also had to deal with data redundancy and duplication. The healthcare sector faced a trend shift towards EHR systems that were designed to combine paper-based and electronic medical records (EMR). These systems were used to store clinical notes and laboratory results in its multiple components [1]. They were proposed to enhance the healthcare records and to provide an efficient system that would transform the state of healthcare sector [3].

Many hospitals throughout the world have adopted EHR systems because of their many advantages, chief among them being increased security and cost-effectiveness. Since they offer a great deal of functionality to the healthcare industry, they are seen as an essential component [4]. These features include lab test results, patient appointment scheduling, billing and accounts, and electronic medical record storage. Many of the EHR systems in use in the healthcare industry have them available. Providing safe, tempered-proof, and scalable medical records across many platforms is the main goal. Although the idea behind using EHR systems in hospitals or other healthcare settings was to improve the quality of care, these systems had certain issues and fell short of the expectations that were placed on them [3]. According to a study done in Finland to learn about the experiences of nursing staff with electronic health records, EHR systems have issues with being unreliable and not being very user-friendly [5]. Other issues that the EHR system encounters are as follows:

Interoperability: It is the method by which various information systems communicate with one another. The data needs to be interchangeable and functional for future uses. Health Information Exchange (HIE) or general data exchange is a significant component of EHR systems. Since different EHR systems are being implemented in different institutions, their technical, functional, and terminological capabilities vary, making it impossible to create a single, globally recognised standard [6]. Additionally, from a technical standpoint, medical records protect patients' safety by reducing errors and facilitating easier access to information [2]. EHR systems were designed to address the issues associated with paper-based exchanges of information. The information that was interpreted might then be used in other ways [6].

Information Asymmetry: Information asymmetry, or one party having better access to information than the other, is regarded by critics as the biggest issue facing the healthcare industry today. Since doctors and hospitals have central access to patient records, the general healthcare sector, including EHR systems, suffers from this issue. A patient must go through a drawn-out and time-consuming procedure in order to access his medical records. Only hospitals or other healthcare organisations have access to the information, which is centralised within a single organisation.

Data Breaches: The healthcare industry's data breaches also highlight the need for an improved platform. According to a study [7] that examined data breaches in EHR systems, since October 2009, 173 million data entries had been compromised in these systems. Hospitals are now targets of cyberattacks, according to a different study by Argaw et al. [8], and the researchers saw a growing trend during this study that indicates a lot of research has been done in this area [9][10] [11].

Furthermore, many EHR systems struggle with issues of inefficiency and inadequate system adaption since they are not built to meet the demands and requirements of patients [12]. The literature also implies that information processing has suffered as a result of the adoption of EHRs [2]. Given these issues, it makes sense to look for a platform—Blockchain, in this case—that could aid in converting the healthcare industry to one that is patient-centered. a platform that offers data integrity for patient medical records while also being safe and transparent.

This study suggests a framework for building such a decentralised platform that would house medical records of patients and grant access to such records to clinicians or patients themselves. Since blockchain is not meant to hold enormous amounts of data, we also plan to address the scalability issue with it. In order to address the scalability issue, we would employ the off-chain scaling technique, which stores the data on the underlying media. Additionally, the goal of our suggested work is to address the information asymmetry and data breaches issues that the EHR system is now facing.

The structure of this document is as follows: This paper's section II provides an overview of blockchain technology and its dependencies, while section III describes the relevant research that has been done in this field. The suggested framework's architecture and design are explained in section IV, and its functionality is explained in section V. The conclusion and references are given in the final section.

II RELATED WORK

Many efforts have been made over time to enhance Cloud Health Records' privacy and security. Several works will be reviewed in this area, with an emphasis on their goals, methods, contributions to the field, and limits. Some of the literature articles I reviewed are listed below:

When Satoshi Nakamoto created blockchain technology [13], the main goal was to create a decentralised, cryptographically secure money that would be useful for financial transactions. Eventually, the concept of blockchain was being applied to a number of other domains, the healthcare industry being one of them. Numerous academics have conducted studies in this field, with the aim of determining the viability of implementing blockchain technology in the healthcare industry. They also list the benefits, risks, issues, and difficulties that come with using this technology. A few researchers also talked about the difficulties in putting this into practice on a bigger scale. kept off-chain. This study included the fundamental concepts and structure for implementing the five off-chain data storage patterns that were described. According to the writers, all data that is kept on the blockchain through transactions is considered on-chain data. Off-chain data storage, on the other hand, involves off-chain data storage—that is, data that is not on the chain and does not contain any transactions.

The review delves into the field of Electronic Health Record (EHR) Management Systems, specifically concentrating on the methods and functions of these systems during major disasters and the ensuing mass crises. Prior to the advent of smart contacts on the blockchain, a sizable portion of the literature was primarily concerned with the frameworks and techniques for exchanging EHRs on cloud infrastructures [14]. A novel method for expressing complicated logic on the blockchain using a Turing-complete language was introduced, which sparked a new line of inquiry into peer-to-peer communication and distribution. Indeed, following Ethereum, a fresh batch of decentralised frameworks and systems have been researched and put out by academic institutions as well as business sectors [15]. These frameworks use a variety of blockchain models, ranging from Ethereum to Corda and Tendermint, which are the later implementations.

The Ethereum public blockchain is being used to construct the prototype. Users' public keys, which are Ethereum addresses, are used for access control, and stakeholders join the network as "miners" by operating nodes. It suggests that in order to communicate with it, each party—including the patient—needs to have a blockchain node. The requirement for each actor in the system to have a complete copy of the data is the primary disadvantage of this implementation. The consensus protocol's limited scalability is a further drawback. Setting the upper restriction to 60 transactions per second is feasible, notwithstanding the authors' lack of mention of this potential cap[16].An overview of blockchain technology, bitcoin, and Ethereum was given by Vujičić et al. [22]. According to the authors, the field of information technology is always evolving, and blockchain technology is helping information systems. They defined bitcoin as a distributed peer-to-peer network that facilitates bitcoin transactions. They also provided definitions for the blockchain mining idea and the proof-of-work consensus algorithm. The authors stress that blockchain technology has serious scaling issues, and they offer several ways to address these issues, such as SegWit and Lightning, Bitcoin Cash, and Bitcoin Gold. The paper elucidated Ethereum and its interdependencies, while also drawing distinctions between the Ethereum and Bitcoin blockchains.

It is important to define the terms Electronic Medical Records (EMR) and Electronic Health Records (EHR) before delving into the past and present research. Although the terms appear to be synonymous and are sometimes used interchangeably, there are two distinct categories of digital recordings. The former can be thought of as the digital version of a practitioner's paper patient record. It includes the patient's medical history, including any diagnoses and treatments administered by a specific doctor. The latter, on the other hand, is a more comprehensive document that contains the whole medical history of the patient and is intended to be shared with other authorised users from A study by Wang et al. [23] concentrated on smart contracts and how they are employed in blockchain technology. They begin by introducing smart contracts together with their operational structure, operating systems, and other key ideas. The authors also go over how the novel idea of parallel blockchains might make use of smart contracts. They conclude that the decentralisation provided by the programming language code embedded in smart contracts is the primary driver behind their use in blockchain technology. The author first covered the fundamentals of smart contracts before going into the several blockchain layers that work together to maintain system functionality. Data, network, consensus, incentive, contract, and application layer are these layers. The paper provides an overview of smart contract architecture and framework, as well as an analysis of its challenges and applications. The study also covers a significant emerging trend in parallel blockchain technology, which aims to build a blockchain capable of optimising two distinct but crucial modules.

Azaria, Ekblaw, et al. are the first to present a completely working prototype utilising blockchain technology in electronic health records [3]. Their proposed system, MedRec, is intended to manage EMRs in a distributed manner in addition to controlling access and authenticating users. Its purpose is to address issues such as fragmentation of health data, slow access, interoperability of systems, patient agency, and increased data quantity and quality for medical research. They describe a system with a modular design intended for integration in an effort to accomplish this. In actuality, the actual medical record is retained off-chain on the hospital's relational database in order to address scalability concerns and promote adoption. Metadata and references to the EHR location are stored on the blockchain To put it another way, a smart contract specifies access rules and pointers to the data while also managing the interaction between actors and the data. The pointer is a tuple that contains the host port and credentials for accessing the EHR, along with a query string to be run on the provider's database [3].In a review, Kuo et al. [24] covered a number of blockchain applications in the biomedical and healthcare industries. The authors noted that there are numerous benefits to using blockchains in this field, including decentralisation, the preservation of clinical or medical records, data pedigree, continuous data accessibility, and, most importantly, the availability of secure information to stakeholders in the biomedical or healthcare industries. It was determined that the following are the drawbacks of blockchain technology: secrecy, speed, scalability, and the possibility of hostile attack, or 51% attack. Since they are being used to hold private medical or clinical records, the authors concluded that these constraints are crucial for the biomedical or healthcare industries. The authors suggested using VPNs (Virtual Private Networks) to protect against malicious assaults, encrypting data to preserve secrecy, and storing sensitive medical data off-chain as solutions to these issues.

Sahoo and Baruah [25], suggested a blockchain framework that is scalable and uses a Hadoop database. They suggested combining the decentralisation offered by blockchain technology with the scalability of the underlying Hadoop database to address the scalability issue with blockchain. The blockchain built on top of this framework has all the necessary blockchain dependencies, but the blocks are kept on the Hadoop database to increase the scalability of the blockchain technology. This is how they saved the blocks. This study suggests using the Hadoop database system in conjunction with SHA3-256 hashing for transactions and blocks to address the scalability issue of the blockchain platform. Java was the programming language utilised to create this architecture. This study helped to clarify how blockchain technology can be applied to other scalable platforms in order to enhance or address the scalability issues with this particular platform.

Regarding the recommendations grounded in public blockchain implementations, Linn and Koo's work [29] and Jiang et al.'s BlocHIE [22] should be mentioned. Linn and Koo deviate from [3]'s work on MedRec and contend that the EMRs need to be kept off-chain in a data lake structure. This is required to achieve scalability since a blockchain that follows the Bitcoin paradigm would cause massive files and extensive record replication across all network nodes, consuming more bandwidth and squandering storage and network resources [29]. Their research focuses on discussing some of the most important interoperability issues facing the healthcare industry and how blockchain technology could be able to help. Additionally, they touch on a few technical solutions regarding data privacy, access security, and scalability. Nevertheless, the writers merely outline some fundamental ideas for a potential work-flow rather than suggesting a brand-new system or providing examples of a design. Moreover, they do not evaluate or explain how it would function; instead, they merely discuss the aspects of fault tolerance and disaster recovery that are connected to replication and the absence of a single point of failure. A scalable approach for the blockchain in clinical records was put up by Zhang et al. [26]. The primary goal of this research was to create an architecture that meets the specifications set out by the Office of National Coordinator for Health Information Technology (ONC). This study found that the primary challenges this technology faces are those pertaining to privacy, the security of blockchain, scalability issues because of the massive volume of datasets being transmitted on this platform, and the lack of an industry standard for data exchange on blockchain. A decentralised application (DAPP) demonstration based on the previously stated ONC requirements' design is also included in this study. They also discussed how to improve the FHIR chain and the lessons learned.

Kim et al. [27] suggested a system to organise medical surveys with the goal of utilising blockchain technology to share data. The objective of the medical questionnaire selection, preservation, and distribution, according to the authors, is to use the data for future clinical and medical research. The authors chose blockchain technology for their suggested framework in part because they felt it would be useful for establishing diagnosis systems, resolving terminologies used in EHR systems, and addressing security challenges related to these systems. There are two primary purposes for this study: to generate, store, and disseminate the data obtained from questionnaires. The system also offers the validation of the questionnaires that are submitted through it. Before being parsed to separate personal data from specific data linked to questionnaire results, the newly added questionnaires are first verified to be in the correct format. By doing this, it would be possible to share data for upcoming studies. The authors also discuss the situation in which a third party asks to view the questionnaire data; in this case, the patient's consent must be requested by the doctor in order for the third party to view the data.

III. THEORETICAL BACKGROUND

As previously mentioned, a decentralised programme known as a blockchain is created when several blocks are linked together in a peer-to-peer network. Hashes of earlier blocks are contained in the header of current blocks. Three elements make up a block: data, the hash of the previous block, and the hash of the current block. Depending on the kind of blockchain, the data could be anything. Similar to bitcoin, the data is made up of coins, which are really electronic money [13]. These blocks' hashes include the SHA-256 cryptographic technique, which is used to uniquely identify each block in the chain.

Blockchain covers a wide range of subjects, tools, and ideas, from distributed systems consensus to security and cryptography, business models, and financial incentives. The goal of this thesis is to present a methodical investigation to demonstrate if blockchain technology could be useful for managing medical data during widespread emergencies. Therefore, to fully grasp the potential benefits of distributed ledger technology as well as any potential problems or downsides, it is crucial to grasp some fundamental ideas in the domains of distributed systems and healthcare. The purpose of the ensuing sections is to elucidate some of the fundamental and sophisticated ideas that underlie blockchain technology, such as the processes that allow for consensus in distributed systems and the distinction between permissioned and permissionless models. To comprehend the reasoning behind selecting one model over another for the management of electronic health records, this distinction must be made. Subsequently, a fairly realistic section on the blockchain system used for the thesis project, Hyperledger Fabric, will be included. A review of previous and current research on the scalability and performance of distributed systems for EHR management completes the theoretical framework.

Blockchain

A chained series of connected blocks serves as the record storage for a blockchain data structure. This sequence is copied in numerous machines known as nodes that communicate with one another to build a distributed ledger. The nodes create a peer-to-peer network in which the network uses a consensus procedure to approve each ledger change. Everyone's opinion of the system's current state is guaranteed to be the same by the consensus process. The technology was first presented in 2008 as the basis for the cryptocurrency known as Bitcoin, with the intention of resolving the issue of double spending [37] and enabling peer-to-peer value exchange without the need for a central authority to mediate transactions. Actually, prior to Bitcoin, there was no way to safely transfer money online between parties without depending on a reliable third party, such banks or credit card companies. In order to replace the requirement for trust with cryptographic proof and consensus, the new coin used security techniques like hashing, public keys, and anonymity [37]. In addition to being distributed, blockchain is by nature safe and resistant to malicious activities, misbehaviour, and node failures (i.e., Byzantine fault tolerant) [37][52]. This and other features made it desirable for a wide range of applications, including supply chain management, medical records and identity management [3], assets insurance, and provenance and anti-counterfeiting for premium products. Numerous industries have begun looking into and releasing this technology onto the market in recent years. However, the primary obstacles stem from this new paradigm's intricacy and the comparatively small number of effective cases. One may argue that there is still a lot of room for innovation.

Active and passive replication in distributed systems

Replication is mostly utilised in distributed systems to offer fault tolerance. Replication specifically comes in two flavours: passive and active. To ensure that every node running the application receives the same end result, deterministic processes are necessary for active, or state machine, replication. Maintaining consistency in the state requires this. Sending the updates to everyone in the same order is another requirement of determinism. An atomic broadcast protocol with delivery assurances makes this possible. Even in the event of Byzantine faults, the system can function effectively thanks to active replication [17]. Passive replication involves a single node, or a subset of nodes, processing a request and updating all other nodes with the new state. Although it tends to be less resilient in the event of errors, passive replication can also be utilised for non-deterministic systems [17].

Blockchain models

A blockchain is an open, distributed network, as was previously explained. This concept typically pertains to a specific model that is referred to as public or permission-less. With no rules limiting access or interaction, anyone can join and leave the public model at any time. Therefore, unless encryption and smart contract logic are used, any data kept on a public blockchain, such as Bitcoin or Ethereum, is available to everybody. Blockchain can be used in a private network where users' identities are known in addition to the public model. Usually, permissioned or consortium refers to this constrained paradigm. The way the network reaches consensus is greatly influenced by the participation model [50].

Permssionless model

Under the permissionless paradigm, anyone can take part, and identities are either anonymous or pseudonymous. Any user can create an address and a set of keys to communicate with other users on the blockchain network. As a result, everyone has the ability to add information to the ledger, read data, and initiate transactions. Installing a blockchain node and taking part in consensus, a method for validating transactions, is also possible with this paradigm. Ethereum and Bitcoin are two instances of such networks. In the latter, users can write and install publicly accessible code, or "smart contracts," that can be invoked by everyone. The smart contract operates in an environment known as the Ethereum Virtual Machine (EVM) and is uniquely identified by its address. An incentive structure is necessary for public and permissionless blockchains to ensure the proper operation and continued survival of the network. Rewards and fees are the forms that the incentives take. For instance, Ethereum includes a built-in currency called ether that acts as a means of paying transaction fees as well as liquidity to facilitate the exchange of value between different kinds of digital assets. In actuality, users have to pay ethers in order to validate their transactions and access smart contract functionality. During the consensus process, which results in an agreement on the new state of the system and the global order, the miners gather the fees. The Proof of Work (PoW) consensus mechanism used by the early permissionless blockchains pits participants, or miners, against one another to solve computationally challenging mathematical puzzles. The ability to reach consensus in a network without formal barriers by replacing them with economic ones is what makes this process interesting. This indicates that a node's contribution to the consensus process is directly correlated with the amount of processing power it is able to generate. Research on performance and scalability shows that current PoW-consensus blockchains may theoretically process 60 transactions per second while maintaining the same level of security [16This restriction is a built-in feature of the consensus protocol and is influenced by block size and frequency. Therefore, PoW is not a good fit for applications that require throughput in the range of thousands of transactions per second and go beyond the original intent of cryptocurrencies. Furthermore, the protocol's energy usage turns out to be quite inefficient. To get around throughput restrictions and excessive energy consumption, new protocols and techniques including Proof of Stake (PoS), Proof of Burn (PoS), and Proof of Elapsed Time (PoET) have been proposed recently [12].

Permissioned and consortium model

A closed system with identified players who are acquainted with one another is called a permissioned blockchain. It is designed to facilitate the safe and effective flow of information inside a group or within an individual organisation. The permissioned model is gaining traction among corporations as evidence that participant anonymity is not always a desirable attribute. This is because the model allows for secure interactions across a network of businesses that have shared aims but lack complete trust in one another [2]. Tendermint, Postchain, and Corda are a few examples of similar models. The Linux Foundation-hosted open-source project Hyperledger Fabric is one of the most well-known works. The architecture of Fabric is extendable and adaptable to accommodate many enterprise use cases. In the aforementioned solutions, membership services—trusted third parties—manage confidentiality and privacy. This service, referred to as the Membership Service Provider in Fabric, is responsible for maintaining every identity within the system. It is in charge of providing the credentials needed for authorization and authentication. Generally speaking, every organisation uses a local version of the service to provide its members with public keys and certificates [2]. Since each message and transaction needs to be signed, the credentials are required in order to engage in network activity. Consequently, this enhances the network's security and privacy for all users. Such systems allow for a new class of consensus techniques based on Byzantine Fault Tolerant (BFT) state machine replication protocols, such as the Practical Byzantine Fault Tolerant (PBFT), despite the fact that identity management in such systems is logically centralised in some way. Hence, consensus implementation is more precise and independent of mining, unlike proof-of-work (PoW) implementation. Furthermore, the notion of consensus is more comprehensive and encompasses the entire transaction process, starting from the proposal and ending with the commit [2][6]. Through both theoretical and practical testing, BFT protocols have proven their capacity to handle tens of thousands of transactions with acceptable network speed latencies. The users of these new implementations are not need to pay for the transaction execution process, nor do they require reliance on an integrated coin. In actuality, a firm pays to join the network, therefore protecting it from harmful behaviour is in their best interest. As a result, neither miners nor incentive models are required. Permissioned blockchains offer superior performance, accountability, transparency, and privacy features, making them a better choice for applications like EHM systems that need to maintain security and privacy while attaining high throughput and scalability.

PBFT Consensus

Byzantine fault-tolerant protocols show the greatest promise for maintaining security in the presence of malfunctioning components in permissioned blockchain networks. But since these protocols were first built on synchronous models, they weren't appropriate for use in network applications. Furthermore, the exponential growth of communication cost with the number of consensus participants impeded the scalability of nodes [51]. Due to these features, BFT algorithms were not as widely used as their crash-tolerant cousins, or Paxos, until the introduction of the practical BFT (PBFT) algorithm in 1999 [8]. By lowering the communication overhead from exponential to polynomial, the technique lowers the total response time. Additionally, it is well suited for systems that communicate via Internet protocols because it is made to function in eventually synchronous contexts [6][8]. The five steps of the algorithm are shown in figure 2:

- **Request**: the client sends a request to the master node.
- **Pre-prepare**: the master node forwards the request to the other nodes which decide whether to accept the request or not.
- **Prepare**: in case the nodes accept the execution, they send a preparation message to all the other nodes. Upon receiving at least 2f +1 messages, the nodes start the commit phase if the majority has accepted the request.

• **Commit**: each node sends a commit message to all the other nodes in the system. When a node receives 2f + 1 commit messages, it executes the logic to fulfill the request because it infers that the majority of the nodes has accepted the request.

• **Reply**: finally, the server node replies to the client that waits until the reception. If any message is delayed, the client triggers a timeout and resends the request to the master node [8].

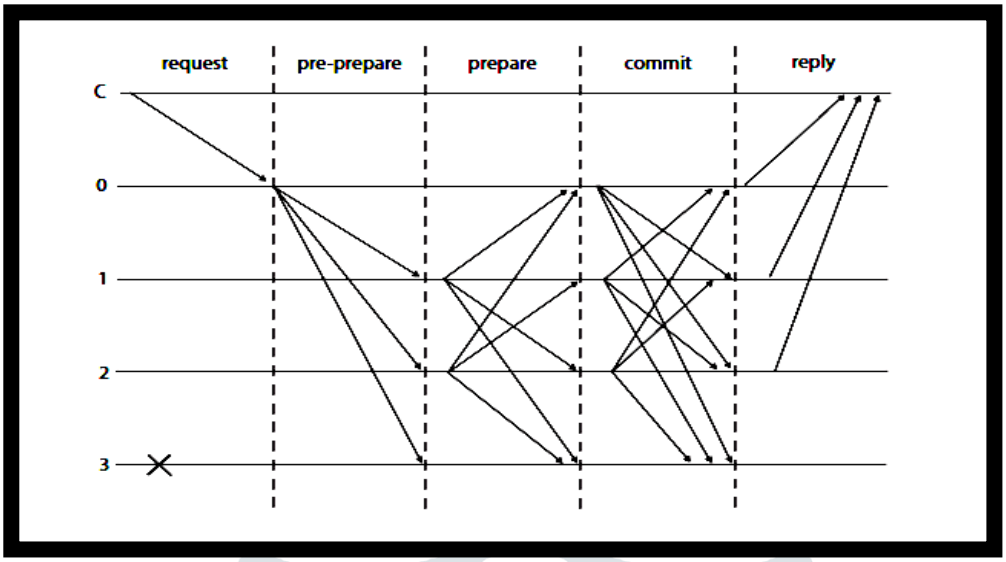


Figure 1 PBFT communication

IV PROPOSED SYSTEM

Blockchain technology is revolutionary and has the ability to revolutionise not just one or two industries but the whole corporate environment. Out of 200 healthcare executives polled, 16% said they planned to use a blockchain solution on a commercial scale this year. Market makers, trade associations, and regulators will be the main players in the implementation of blockchain technology. Supply chain management and healthcare data management and security are two excellent examples of key ideas affecting and being impacted by potential blockchain implementation. Let's examine each of them in brief:

- **Healthcare:** Improved data exchange across healthcare practitioners increases the likelihood of correct diagnoses, improves the efficacy of treatments, and generally enables healthcare organisations to provide care at a lower cost. By tracking the provenance of data and any modifications made, blockchain technology can help different stakeholders in the healthcare value chain share access to their networks without jeopardising the security and integrity of the data.
- **Health Chain Management:** The ability to monitor transactions more securely and transparently is one of the features of blockchain technology that is most applicable to Merkle Hash Trees. Blockchain technology makes it possible to permanently record transactions in a decentralised record, cutting down on expenses, delays, and human error.Data managed by medical organizations includes:
    - Patient health information (PHI);
    - Cloud Health Records;
    - Data collected from monitoring systems.

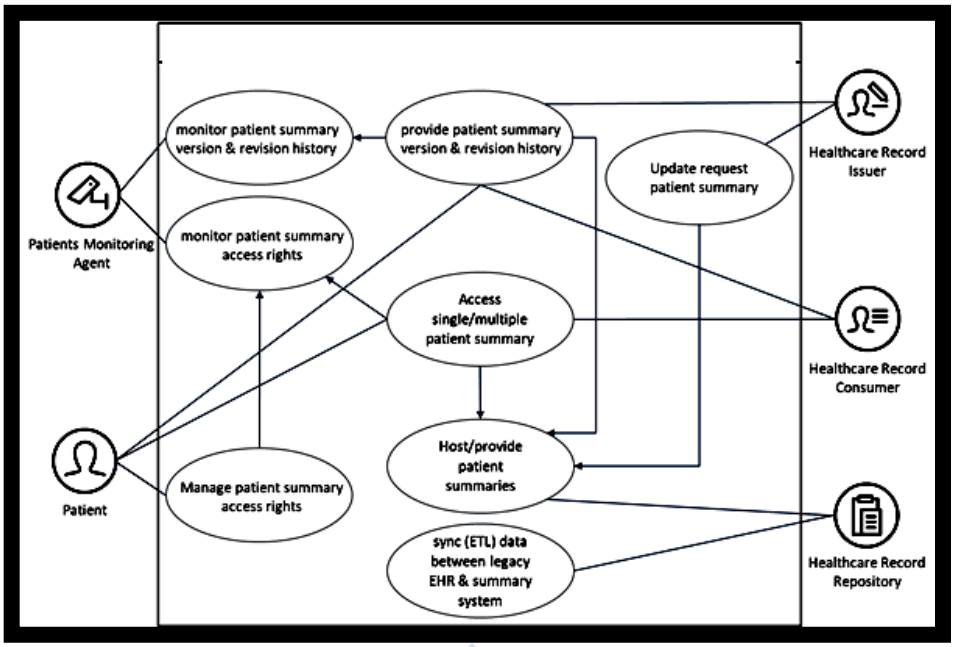


Figure 2 Proposed System Architecture

Health care industry on security:

The two most frequent worries expressed by businesses about the information shared between various entities in the current system are security and trust. Trust problems arise when information can be entered anywhere in a communication channel, particularly in the healthcare sector. Concerns exist over numerous suppliers holding unvalidated versions of the same patient information, which can lead to a variety of inaccuracies, inconsistencies, and incompleteness. It makes sense that healthcare professionals would be concerned given the constant threat of hacking, stories of security breaches, and data manipulation.

Blockchain technology may be the solution to most of these issues because it is cryptographically secure and allows data to be authenticated using individual digital signatures.

Steps for Smart contact between Admin, Doctor and Patient

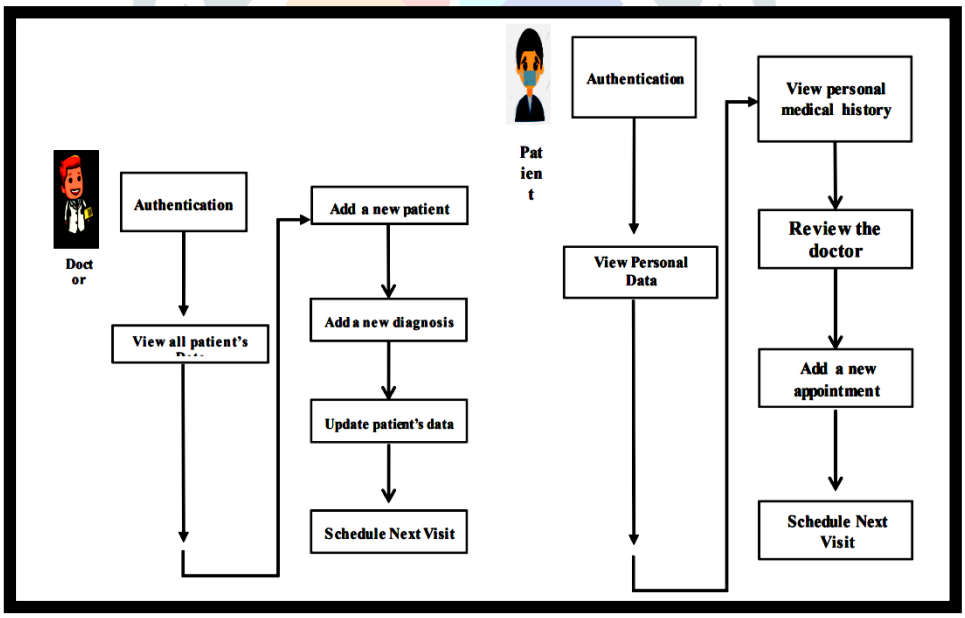


Figure 3 Architecture Diagram

V RESULT ANALYSIS

Testing a decentralised system—or any system with multiple autonomous components—is a difficult task for a number of reasons. First, it takes time and effort to start up and initialise components on different machines. Secondly, communication links can break during the execution process. Third, different components may only present failures when operating in a specific order. Finally, when something goes wrong, it's frequently necessary to examine the interactions and history of all the connected components. In particular, since representative indicators are still being discussed in the literature and testing tools are still in the early stages of development, evaluating the security and performance of a blockchain network presents unique issues. Because experimental validation is not always complete, the literature's approach to security is typically focused on modelling, trust assumptions, and theoretical evaluations. However, analysing the performance presents additional difficulties because test suits must be designed to reach every component and replicate a real-world environment in which every component is under pressure. The methods, metrics, and tools used to assess the prototype's performance for electronic health records are covered in the section that follows. Following that, the performance test results will be shown.

Approach and tools

The blockchain for EHRs prototype, constructed with HL Fabric, includes two primary states, which switch to each other in the event of an emergency, as was described in the preceding chapters. To determine whether the prototype can be useful for managing health records with ease and security preservation, it is required to examine its behaviour and performance. A decentralised system can be tested in a variety of ways, but the natural method selected for this prototype is based on the system's presentation of two distinct states. In actuality, the system can be analysed statically or dynamically depending on the statesIn the first scenario, the prototype is tested in its regular state first, and then it is tested in its emergency state. The various environments and configurations yield varying results, which are subsequently examined and contrasted to gain understanding that informs the examination of the prototype and the elements influencing the performances. In the latter scenario, examining the change from one state to another can provide a dynamic picture of the system.

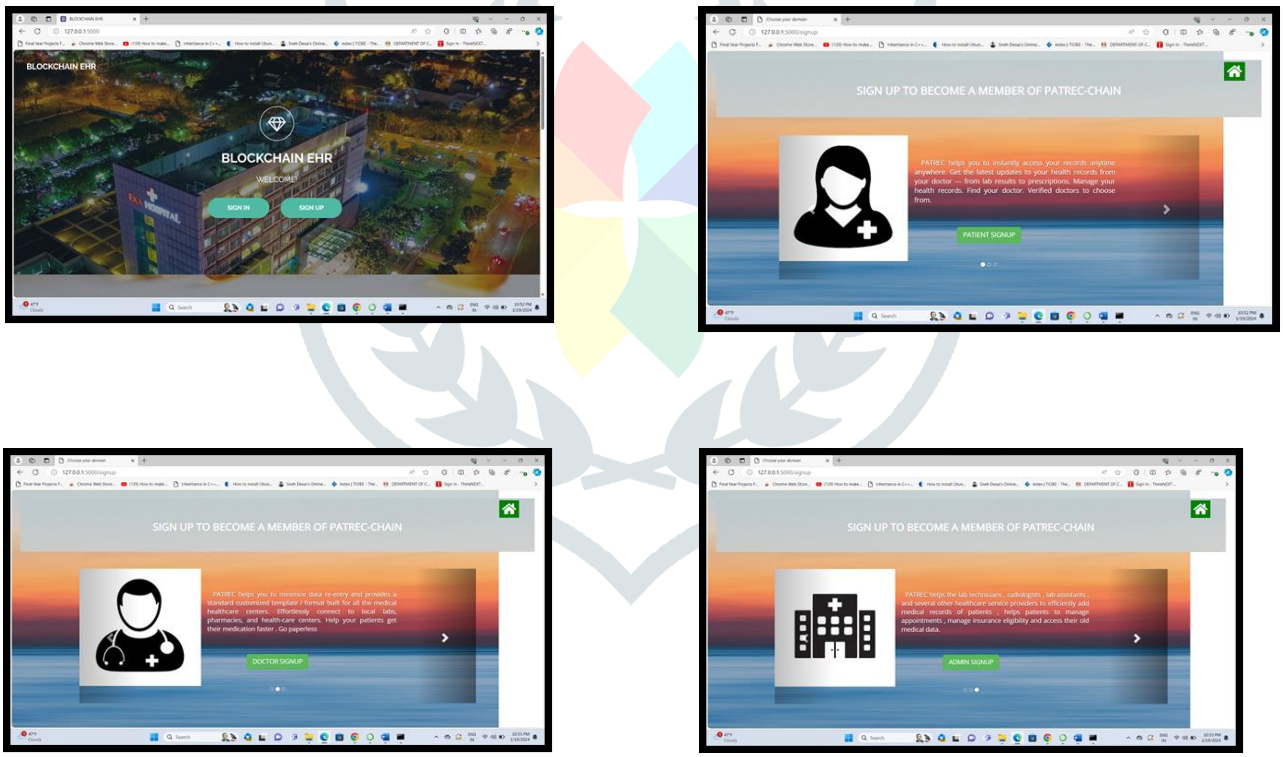
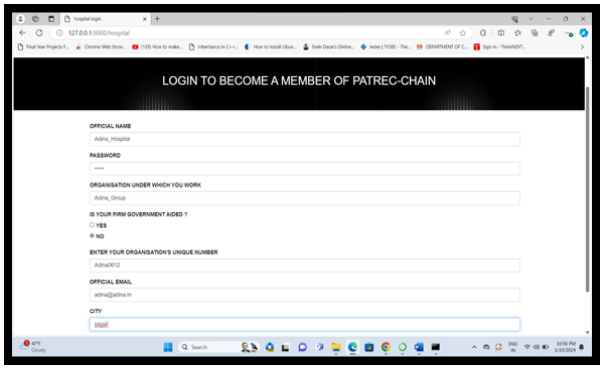
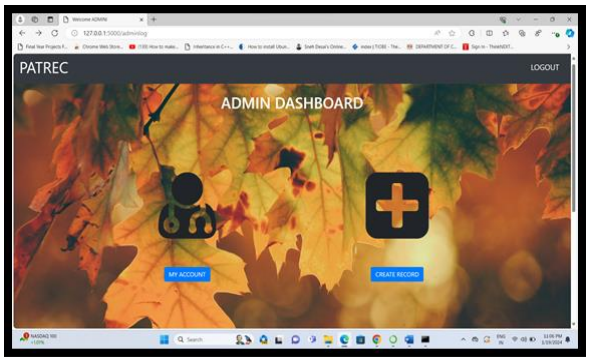
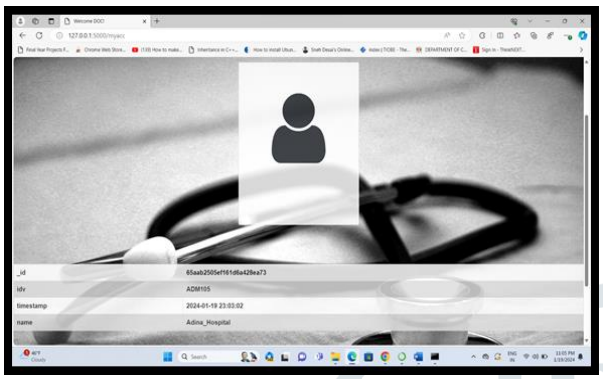
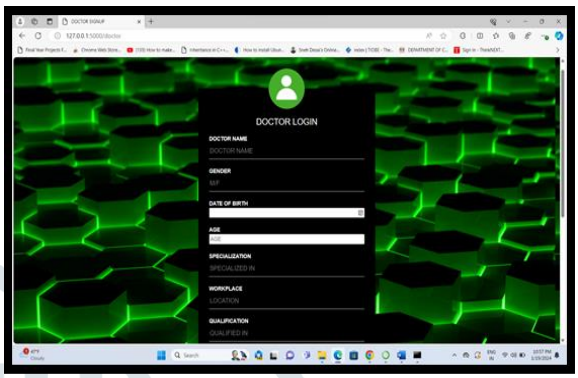


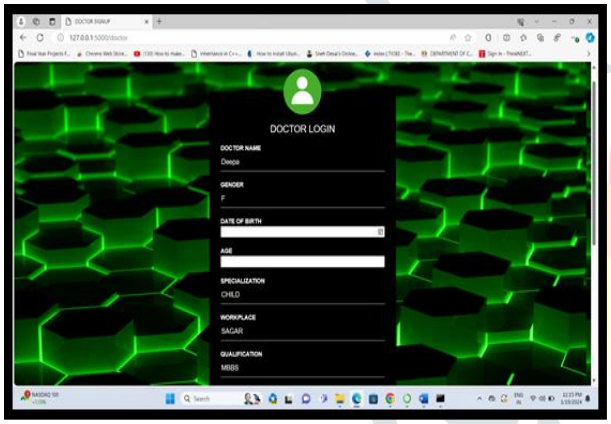
Figure 4 Dashboard of Doctor Login

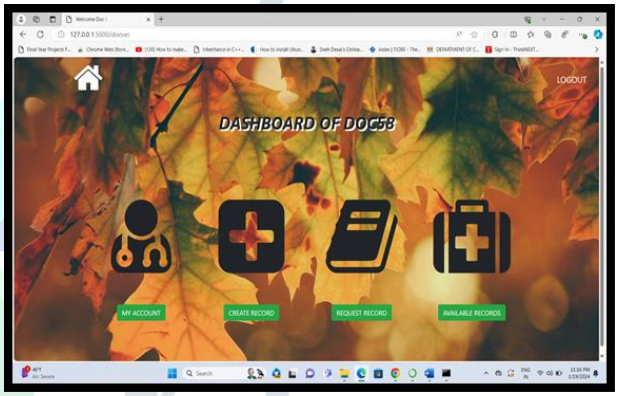

LOGIN TO BECOME A MEMBER OF PATREC-CHAIN
OFFICIAL NAME
PASSWORD
ORGANISATION UNDER WHICH YOU WORK
IS YOUR FIRM GOVERNMENT AIDED ?
YES
NO
ENTER YOUR ORGANISATION'S UNIQUE NUMBER
OFFICIAL EMAIL
CITY

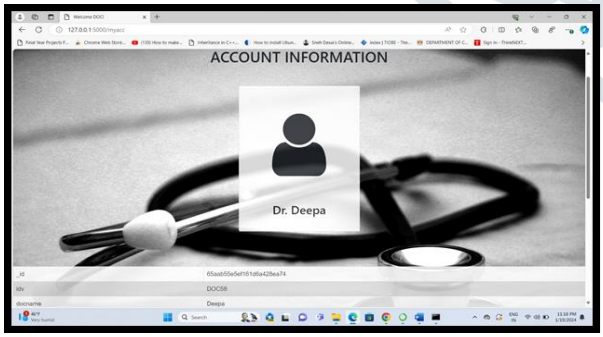

PATREC
LOGOUT
ADMIN DASHBOARD
MY ACCOUNT
CREATE RECORD

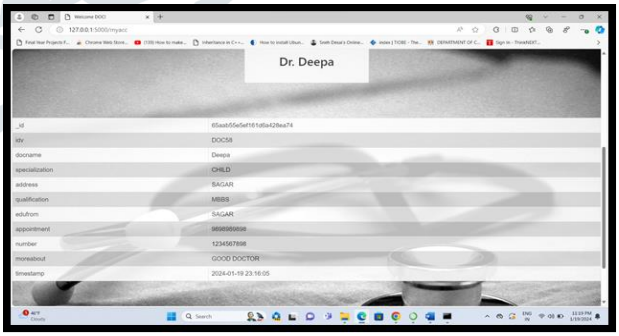

_id
idv
timestamp
name


DOCTOR LOGIN
DOCTOR NAME
GENDER
DATE OF BIRTH
AGE
SPECIALIZATION
WORKPLACE
QUALIFICATION

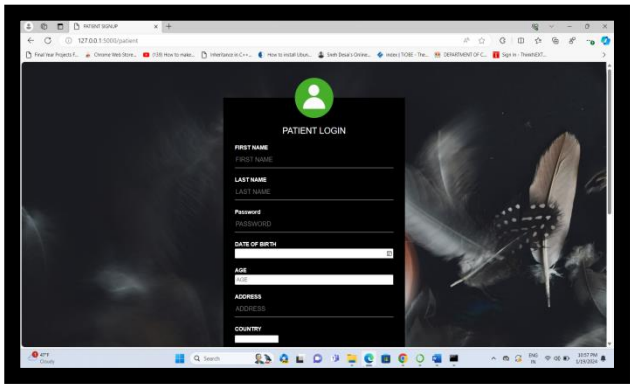

DOCTOR LOGIN
DOCTOR NAME
Deepa
GENDER
F
DATE OF BIRTH
AGE
SPECIALIZATION
CHILD
WORKPLACE
SAGAR
QUALIFICATION
MBBS


LOGOUT
DASHBOARD OF DOC58
MY ACCOUNT
CREATE RECORD
REQUEST RECORD
AVAILABLE RECORDS

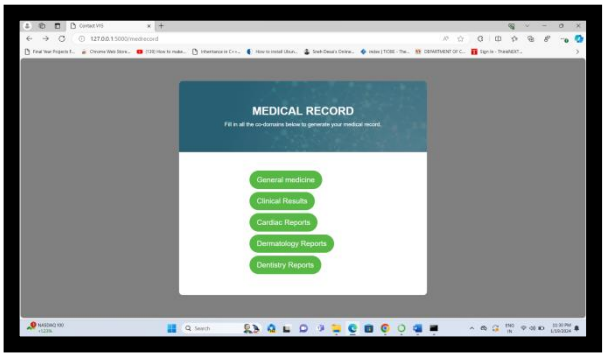

ACCOUNT INFORMATION
Dr. Deepa


Dr. Deepa

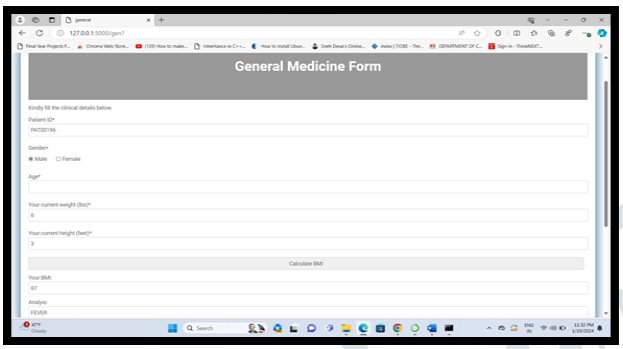
Sign up Patient with using Necessary Details.



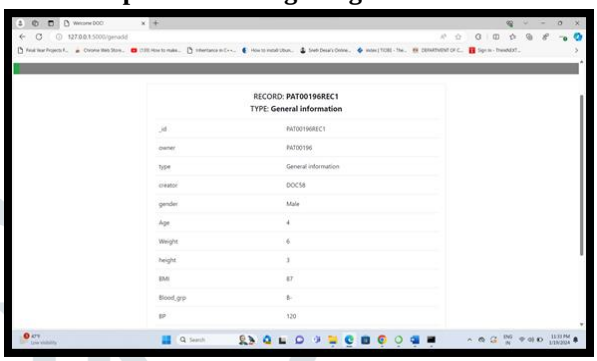
Doctor get the details of patient and prescribe medicine.



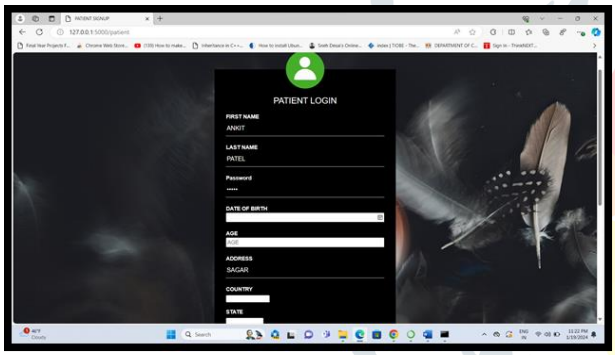
Doctor used patient ID for getting his/her information.



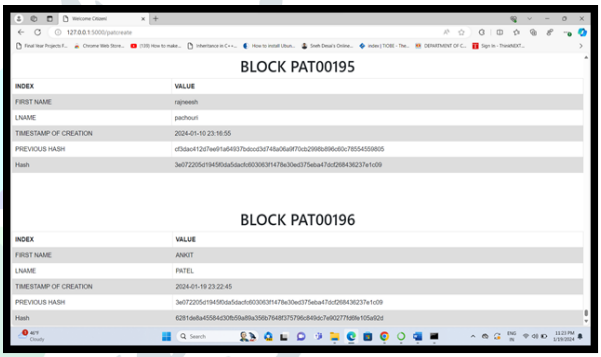
Doctor used patient ID for getting his/her information



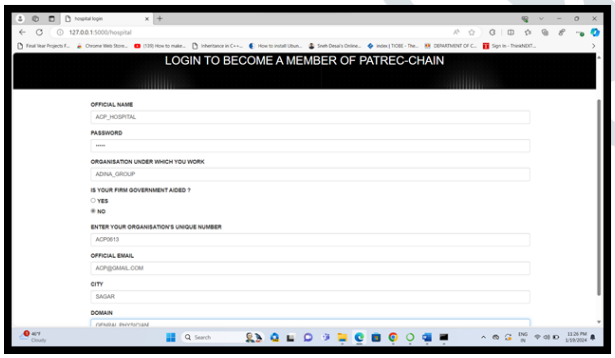
patient Login with Block



Patient information saved in block chain.



Patient information saved in block chain



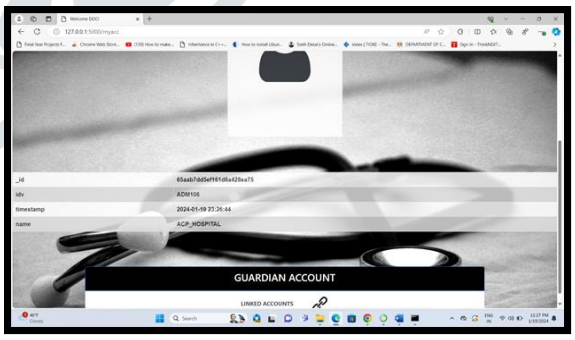


Figure 6 Patient information saved in block chain

VI CONCLUSION

The patient has lifetime access to and secure usage of their report through the EHR system. The patient's private key is used, and it can be used to access the reports going forward. A person lacking the private key is unable to participate in the data retrieval procedure. As a result, patient health records are better protected by BlockChain and may be accessed by the patient using their own private key for future reference. The challenge of acquiring Ethereum units is currently a major barrier to using the network. Units can be earned by mining or bought using fiat money or cryptocurrencies like Bitcoin. We have created a web application user interface for the health record system. Once Ethereum tokens are available, publishing and executing smart contracts is really easy. We can use some distinctive identification attributes to add account authentication elements for enhanced security.

References

[1] G. Jetley and H. Zhang, “Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,” *Decis. Support Syst.*, pp. 113–137, 2019.
[2] K. Wisner, A. Lyndon, and C. A. Chesla, “The electronic health record’s impact on nurses’ cognitive work: An integrative review,” *Int. J. Nurs. Stud.*, vol. 94, pp. 74–84, 2019.
[3] M. Hochman, “Electronic Health Records: a ``Quadruple Win,'' a ``Quadruple Failure,'' or Simply Time for a Reboot?,” *J. Gen. Intern. Med.*, vol. 33, no. 4, pp. 397–399, Apr. 2018.
[4] Q. Gan, “Adoption of Electronic Health Record System : Multiple Theoretical Perspectives,” *2014 47th Hawaii Int. Conf. Syst. Sci.*, pp. 2716–2724, 2014.
[5] T. Vehko *et al.*, “Experienced time pressure and stress: electronic health records usability and information technology competence play a role,” *BMC Med. Inform. Decis. Mak.*, vol. 19, no. 1, p. 160, Aug. 2019.
[6] M. Reisman, “EHRs: The Challenge of Making Electronic Data Usable and Interoperable.,” *P T*, vol. 42, no. 9, pp. 572–575, 2017.
[7] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, “Electronic Health Record Breaches as Social Indicators,” *Soc. Indic. Res.*, vol. 141, no. 2, pp. 861–871, 2019.
[8] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, “The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,” *BMC Med. Inform. Decis. Mak.*, vol. 19, no. 1, pp. 1–11, 2019.
[9] A. McLeod and D. Dolezel, “Cyber-analytics: Modeling factors associated with healthcare data breaches,” *Decis. Support Syst.*, vol. 108, pp. 57–68, 2018.
[10] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, 2018.
[11] “The Future of Health Care Cybersecurity,” *J. Nurs. Regul.*, vol. 8, no. 4, Supplement, pp. S29–S31, 2018.
[12] D. Spatar, O. Kok, N. Basoglu, and T. Daim, “Adoption factors of electronic health record systems,” *Technol. Soc.*, vol. 58, no. February, p. 101144, 2019.
[13] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electrnic Cash System,” pp. 1–9, 2008.
[14] Manas Ranjan Patra, Rama Krushna Das, and Rabi Prasad Padhy. “CRHIS: cloud based rural healthcare information system”. en. In: ACM Press, 2012, p. 402. ISBN: 978-1-4503-1200-4.
[15] Nir Menachemi and Collum. “Benefits and drawbacks of electronic health record systems”. en. In: Risk Management and Healthcare Policy (May 2011), p. 47. ISSN: 1179-1594. DOI: 10.2147/RMHP.S12985.
.
[16] A. Boonstra, A. Versluis, and J. F. J. Vos, “Implementing electronic health records in hospitals: a systematic literature review,” *BMC Health Serv. Res., vol. 14, no. 1, p. 370, Sep. 2014.*
[17] T. D. Gunter and N. P. Terry, “The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions,” *J. Med. Internet Res.*, vol. 7, no. 1, pp. e3–e3, Mar. 2005.
[18] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. June, pp. 557–564, 2017.
[19] C. Pirtle and J. Ehrenfeld, “Blockchain for Healthcare: The Next Generation of Medical Records?,” *J. Med. Syst.*, vol. 42, no. 9, p. 172, Aug. 2018.
[20] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives,” *Cryptography*, vol. 3, no. 1, p. 3, 2019.
[21] J. Eberhardt and S. Tai, “On or Off the Blockchain? Insights on Off-Chaining Computation and Data,” *Smart SOA Platforms Cloud Comput. Archit.*, no. October, pp. 11–45, 2014.
[22] D. Vujičić, D. Jagodić, and S. Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” *2018 17th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2018 - Proc.*, vol. 2018-Janua, no. March, pp. 1–6, 2018.
[23] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, “An Overview of Smart Contract: Architecture, Applications, and Future Trends,” *IEEE Intell. Veh. Symp. Proc.*, vol. 2018-June, no. Iv, pp. 108–113, 2018.
[24] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.
[25] M. S. Sahoo and P. K. Baruah, “HBasechainDB -- A Scalable Blockchain Framework on Hadoop Ecosystem,” in *Supercomputing Frontiers*, 2018, pp. 18–29.
[26] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain : Applying Blockchain to Securely and Scalably Share Clinical Data,” *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.
[27] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, “Sharing Medical Questionnaries based on Blockchain,” *Proc. - 2018 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2018*, pp. 2767–2769, 2019.
[28] S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," Decentralized Bus. Rev., White Paper, Oct. 2008, Art. no. 21260. [Online]. Available: https://www.debr.io/article/21260-bitcoin-a-peer-topeer- electronic-cash-system
[29] V. Buterin, ``A next-generation smart contract and decentralized application platform," White Paper, 2014, vol. 3, no. 37. [Online]. Available: https://nft2x.com/wp-content/uploads/2021/03/EthereumWP.pdf
[30] W. Vaugan, J. Bukowski, and S. Wilkinson. (2016). *Chainpoint: A Scalable Protocol for Anchoring in the Blockchain and Generating Blockchain Receipts*. Accessed: Dec. 14, 2021. [Online]. Available: https://bit.ly/33s2CRM.
[31] A. Guo, ``Blockchain receipts: Patentability and admissibility in court," *Chicago-Kent J. Intellectual Property*, vol. 16, no. 2, p. 440, 2017.
[32] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J.-N. Liu, Y. Xiang, and R. H. Deng, ``CrowdBC:Ablockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251_1266, Jun. 2018.