International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Confidentiality of Patience Medical Record Using Blockchain

Mr Shankar J[1], Shravani S M[2], Singam Suresh Reddy[3], Preethi Rajagopalan[4]

[1]Assistance Professor, [2,3,4]UG Student Computer Science (CSE)
School of Computer Science (Blockchain), Bangalore Presidency University
[1]shankar.j@presidencyuniversity.in, shravanism2802@gmail.com[2], singamreddysureshreddy@gmail.com[3], preethi111102@gmail.com[4]

ABSTRACT

Blockchain has been a focal point of research across diverse industries for an extended period, demonstrating its utility in various applications. Within the healthcare sector, the integration of blockchain technology holds immense potential, offering advantages such as enhanced security, privacy, confidentiality, and decentralization. Despite these benefits, Electronic Health Record (EHR) systems encounter challenges related to data security, integrity, and effective management.

This paper explores the transformative potential of blockchain technology in addressing the issues faced by EHR systems. A proposed framework is presented, offering a structured approach for implementing blockchain technology in the healthcare sector, specifically tailored for EHR. The primary objectives of this framework include the incorporation of blockchain into EHR systems and the establishment of a secure electronic record storage system. To fortify security measures, the framework defines granular access rules, ensuring that only authorized users possess the necessary permissions to access sensitive medical information.

Moreover, the framework delves into the broader scalability challenges associated with blockchain technology. It introduces a solution by advocating for the utilization of off-chain storage for records. This strategic use of off-chain storage not only addresses scalability concerns but also optimizes the overall performance of the system. In essence, the proposed framework strives to provide EHR systems with the advantages of a scalable, secure, and integral blockchain-based solution.

Keywords: Blockchain, Solidity, Medical Records, Confidentiality, Node.js, IPFS, Truffle, Ganache, MetaMask.

I. Introduction

The recent surge in technological advancements is reshaping every facet of human existence, revolutionizing our interactions with the world. This transformative wave is not only evident in various sectors but is also making significant strides in improving the healthcare landscape. Technological progress, particularly in Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems, offers substantial benefits such as enhanced security, user experience, and overall efficiency within the healthcare sector. Despite the advantages introduced by EHR and EMR systems, challenges persist in areas like the security of medical records, user ownership of data, and data integrity. One promising solution to these issues lies in the adoption of blockchain technology, which promises a secure and tamper-proof platform for storing medical records and other healthcare-related information. In the pre-modern technology era, healthcare relied on a paper-based system for storing medical records, using manual handwritten mechanisms. This approach proved inefficient, insecure, and prone to disorganization, lacking the crucial attribute of being tamper-proof. Moreover, it encountered challenges related to data duplication and redundancy, as each institution maintaining patient records had its copies. The evolution of healthcare records saw a significant shift towards EHR systems, combining elements of paper-based and electronic medical records (EMR). [1]These systems were designed to store clinical notes, laboratory results, and other critical information with the aim of improving patient safety, preventing errors, and increasing information accessibility. However, despite their intended benefits, EHR systems encountered challenges in addressing the issues inherent in paper-based healthcare records.[2]The global implementation of EHR systems in numerous hospitals underscores their perceived value, particularly in enhancing security and cost-effectiveness. Regarded as a vital component of the healthcare sector,[3] EHR systems offer various functionalities, including electronic storage of medical records, patient appointment management, billing and accounts, and lab tests. Despite their widespread adoption, the primary focus remains on providing secure, tamper-proof, and easily shareable medical records across different platforms.

Despite the initial expectations associated with the adoption of EHR systems to improve healthcare quality, they faced challenges. A study conducted in Finland examined the experiences of nursing staff with EHR systems, revealing issues related to reliability and poor user-friendliness.[4] These problems, alongside others, have prompted a reevaluation of the effectiveness of EHR systems in meeting the expectations set for them in the healthcare sector.[3]

A. INTEROPERABILITY

Interoperability serves as the crucial mechanism enabling different information systems to share data seamlessly. The shared information must not only be capable of being exchanged but also must be designed for usability in subsequent applications. Within the realm of Electronic Health Record (EHR) systems, a significant dimension is the Health Information Exchange (HIE), representing the broader aspect of data sharing.[5] As numerous hospitals deploy diverse EHR systems, the absence of a universally defined standard becomes evident due to variations in terminologies, technical specifications, and functional capabilities across these systems.

The landscape of EHR systems is marked by the deployment of varied terminologies, technical features, and functional capabilities in different hospital settings, contributing to the absence of a universally defined standard. This diversity poses challenges to achieving a seamless exchange of information and hinders the establishment of a unified standard across the healthcare sector. Additionally, at a technical level, the medical records being exchanged should possess interpretability, ensuring that the shared information is understandable and can be effectively utilized. The interpretability of medical records is a crucial factor in facilitating the smooth exchange of information among different EHR systems.[5]

B. INFORMATION ASYMMETRY

Critics argue that the most significant challenge in the healthcare sector today is information asymmetry, a situation where one party possesses better access to information than the other. This issue is particularly pronounced in Electronic Health Record (EHR) systems and the broader healthcare sector, where doctors and hospitals hold centralized access to patient records. This centralization creates a scenario where patients face obstacles in accessing their medical records, requiring them to navigate a lengthy and cumbersome process.Within the healthcare sector, especially in the context of EHR systems, a notable concern raised by critics is the prevalence of information asymmetry. This imbalance arises because doctors and hospitals retain exclusive access to patient records, establishing a centralized control structure. Consequently, patients encounter challenges when attempting to retrieve their medical records, being subjected to a protracted and intricate process for access. The issue lies in the concentration of information within a single healthcare organization, limiting control solely to hospitals or relevant organizations.

C. DATA BREACHES

The imperative to address data breaches in the healthcare sector underscores the pressing need for an improved platform. A comprehensive study [6] scrutinized data breaches in Electronic Health Record (EHR) systems, revealing a staggering compromise of 173 million data entries since October 2009. Another research effort by Argaw et al [7]highlighted the escalating trend of cyber-attacks targeting hospitals, indicating a growing concern in the research community.[8]

Adding to the challenges, numerous EHR systems fall short in meeting patient needs, grappling with inefficiency and poor adaptability [9] Literature further points to negative consequences on information processing resulting from EHR use [2], [9] In response to these issues, there is a rationale for seeking a transformative platform for healthcare that prioritizes patients—enter Blockchain. This proposed platform aims to be secure, transparent, and ensures data integrity in the storage of patients' medical records.This paper introduces a framework that establishes a decentralized platform for storing patient records, granting access to providers and concerned individuals, notably the patients themselves. Addressing the inherent scalability challenge of blockchain, which isn't inherently designed for massive data storage, the proposed framework adopts an off-chain scaling method. This method leverages the underlying medium to circumvent scalability issues by storing data on that medium. Additionally, the framework aims to resolve information asymmetry and data breach problems commonly faced by EHR systems.The organization of this paper unfolds as follows: Section II delves into the fundamentals of blockchain technology and its dependencies. Section III provides a comprehensive overview of related work in this domain. The design and architecture of the proposed framework are expounded in Section IV, followed by a discussion of its performance in Section V. The paper concludes with Section VI offering insights and references.

II. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES

Nakamoto, in his seminal work on digital currency, Bitcoin, introduced blockchain technology as a solution to the double spending problem [10] Originally devised for cryptocurrency, this innovative technology quickly found applications in various domains beyond its initial use case.At its core, blockchain is a continuously expanding chain of interconnected blocks that store transactions. Nakamoto's decentralized approach ensures that information is distributed, and each piece of data has shared ownership. Operating on a peer-to-peer network, blockchains secure batches of transactions through hashing, providing inherent security to the information they contain. The decentralized nature of blockchain offers advantages such as security, anonymity, and data integrity, all without the need for third-party intervention. This makes it a compelling choice for storing patient medical records, especially as advancements in healthcare technology prioritize the security of patient data.In the healthcare sector, where safeguarding patient information is of utmost importance, blockchain's attributes make it a logical and secure option. Numerous researchers echo this sentiment, identifying blockchain technology as a feasible and innovative solution for healthcare applications [11]

A. ARCHITECTURE

1.The image shows a system for storing and managing medical records using a decentralized application (DApp) on a blockchain. In this system, medical records are stored on a distributed ledger, rather than on a central server. This means that the records are not controlled by any one person or organization, and they are accessible to anyone who has the authorization to view them.

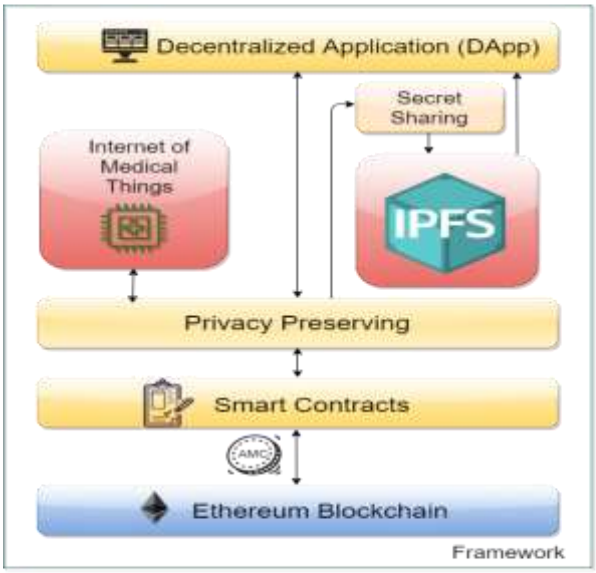

Figure 1. System for storing and managing medical records

The DApp uses smart contracts to automate the process of storing and managing medical records. Smart contracts are self-executing contracts that are stored on the blockchain. They can be used to define the rules for how medical records are shared and accessed.

The system also uses privacy-preserving techniques to protect the confidentiality of medical records. These techniques can be used to encrypt the records or to store them in a way that makes it difficult for unauthorized people to access them.

The Internet of Medical Things (IoMT) is also shown in the image. The IoMT refers to medical devices that are connected to the internet. These devices can collect and transmit data about a patient's health. The data from IoMT devices can be stored on the blockchain using the DApp.

This system has the potential to improve the security and privacy of medical records. It can also make it easier for patients to share their medical records with authorized healthcare providers.

2. The diagram shows how a patient can consult with a doctor through a secure platform. The platform stores the consultation records on a decentralized network called IPFS, which ensures that the records are tamper-proof and cannot be controlled by any single entity.

The platform also allows patients to upload their medical records, such as X-rays and blood test results, which can be viewed by the doctor.

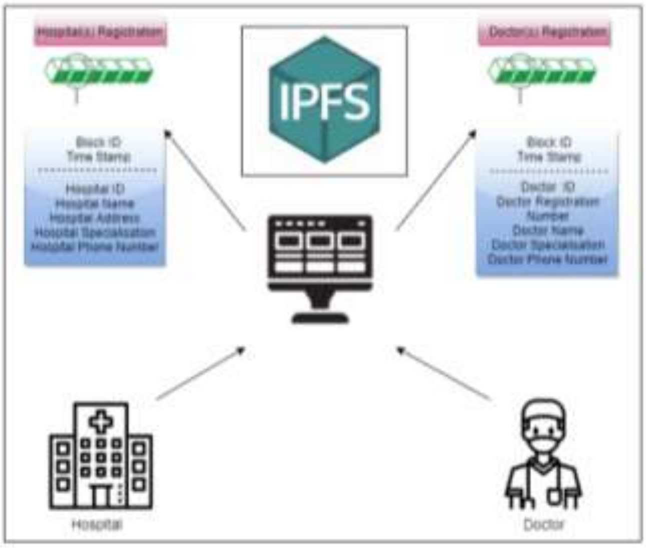

Figure 2. Patient consult doctor in secure platform.

This streamlined approach, where patients consult, doctors diagnose, and labs contribute, all within a unique, secure, and decentralized ecosystem, redefines healthcare, placing the power of information and informed decisions firmly in the hands of both patients and medical professionals.

B. ALGORITHM DETAILS

Securing patient medical records using blockchain involves several key components:

Decentralized Storage: Blockchain allows for decentralized storage of medical records, preventing a single point of failure. Each block in the chain contains a record, and the decentralized nature enhances security.

Cryptography: Blockchain uses cryptographic techniques for secure data storage. Patient information can be encrypted and linked to the patient's private key, ensuring that only authorized individuals can access the data.

Consensus Mechanism: Implementing a robust consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensures that any changes to the medical records require agreement from the network, enhancing the integrity of the data.

Smart Contracts: Smart contracts can be utilized to enforce access controls and permissions. Only authorized parties with the correct cryptographic keys can execute smart contracts to access specific medical records.

Permissioned Blockchain: Implementing a permissioned blockchain restricts access to the network, allowing only authorized participants (hospitals, clinics, healthcare providers) to join. This adds an additional layer of security.

Immutable Ledger: The immutability of blockchain ensures that once a record is added, it cannot be altered. This feature enhances the integrity and authenticity of patient medical records.

Private Transactions: Implementing privacy features, such as zero-knowledge proofs or ring signatures, can add an extra layer of confidentiality by masking the identities of the transacting parties.

These above are the algorithm details which is widely used in blockchain technology for patience medical Record.

III. RELATED WORK

Nakamoto [10]designed blockchain technology with the initial goal of creating a cryptographically secured and decentralized currency for financial transactions This concept has transcended its original purpose and found application in various fields, including healthcare. Researchers have extensively explored the feasibility of integrating blockchain into the healthcare sector. Their studies assess advantages, threats, and challenges associated with this technology, with some discussions on the practical challenges of implementing it on a larger scale.

A. THEORETICAL/ANALYTICAL BLOCKCHAIN-BASED RESEARCH

Gordon and Catalini's study [11] focused on the transformative potential of blockchain in healthcare, highlighting data sharing as a key driver for its adoption. They outlined four critical aspects requiring transformation in the healthcare sector: digital access rights, data availability, faster access to clinical records, and patient identity. The study also addressed on-chain and off-chain data storage, discussing challenges such as the volume of clinical records, security, privacy, and patient engagement. Eberhardt and Tai [12] explored solutions to blockchain scalability, presenting five patterns for off-chain data storage. They defined on-chain data as that stored on the blockchain through transactions, while off-chain data storage involves placing data elsewhere without transactions. The study aimed to identify approaches to solve the scalability problem and shed light on projects addressing this issue.

Vujičić et al.'s overview [13] delved into blockchain, bitcoin, and Ethereum, emphasizing the changing information technology landscape. They discussed scalability challenges in blockchain and proposed solutions like SegWit, Lightning, Bitcoin Cash, and Bitcoin Gold. The authors provided insights into Ethereum's dependencies and differentiated its blockchain from bitcoin's.

Wang et al.'s study centered on smart contracts and their application in blockchain.[14] They introduced smart contracts, their working framework, and their application in parallel blockchains. The paper discussed the architecture, framework, applications, and challenges of smart contracts, highlighting the future trend of parallel blockchains.

Kuo et al.'s review [15]explored diverse applications of blockchain in biomedical and healthcare sectors. The authors highlighted advantages such as decentralization, data persistence, data pedigree, continuous data accessibility, and secure information sharing. Limitations included confidentiality, speed, scalability, and the threat of malicious attacks. Solutions proposed involved off-chain storage for sensitive medical data, encryption for confidentiality, and the use of VPNs for protection against malicious attacks.

B. PROTOTYPE/IMPLEMENTATION BLOCKCHAIN-BASED RESEARCH

Sahoo and Baruah [16]proposed a scalable blockchain framework using the Hadoop database to address scalability issues. They utilized the scalability of Hadoop in conjunction with the decentralization of blockchain, storing blocks on the Hadoop database to enhance scalability. This study suggests that combining blockchain with other scalable platforms, such as Hadoop, can improve and address scalability concerns.

Zhang et al. [17] introduced a scalable solution for blockchain in clinical records, aligning with the Office of National Coordinator for Health Information Technology (ONC) requirements. Identified barriers include privacy concerns, blockchain security, scalability issues related to large datasets, and the absence of a universal standard for data exchange on the blockchain. The study includes a demonstration of a decentralized application (DAPP) based on ONC requirements, addressing lessons learned and proposing improvements for the FHIR chain.

Kim et al. proposed a blockchain-based system for managing medical questionnaires, emphasizing data sharing for medical and clinical research purposes. The system's main functions include creating, storing, and sharing questionnaire data, with added benefits such as validation of submitted questionnaires and ensuring patient permission for third-party access. The authors suggest that their framework can contribute to developing diagnosis systems, resolving EHR terminology, and addressing security issues in healthcare systems.

1.BLOCK

As previously elucidated, blockchains are constructed by interlinking numerous blocks within a peer-to-peer network, culminating in the creation of a decentralized application. These blocks possess headers containing hashes of antecedent blocks, encompassing three essential components: data, the hash of the current block, and the hash of the preceding block. The nature of the data encapsulated within a block is contingent upon the specific type of blockchain in question. In the case of Bitcoin, for instance, the data pertains to electronic cash in the form of coins. [10]The hashes embedded in these blocks employ the SHA-256 cryptographic algorithm, facilitating the distinctive identification of each block within the chain.

2. CONSENSUS ALGORITHM

The seamless addition of each block to the blockchain necessitates adherence to predefined consensus rules, a requirement addressed through consensus algorithms in blockchain technology. A prevalent and foundational example is the Proof of Work (PoW) algorithm, initially introduced by Nakamoto [10]in the Bitcoin network. The operational mechanism involves nodes or participants in the blockchain network, where the initiation of a transaction prompts a computational process known as mining. Nodes engaged in these calculations, referred to as miners, play a pivotal role in validating and adding transactions to the blockchain.[18]

3. KEY FEATURES OF BLOCKCHAIN

A.DECENTRALIZATION

The distinctive characteristic of decentralization in blockchain manifests as the dispersion of information across the network rather than centralized at a singular point. This decentralization model facilitates consensus-based control and management of information through collective input from interconnected nodes. The transition from concentrated control to a distributed paradigm ensures that data, once confined to a central point, is now entrusted to multiple reliable entities.

B.DATA TRANSPARENCY

In the technological realm, achieving data transparency necessitates fostering a trust-based relationship among entities. Blockchain addresses this imperative by distributing data or records across the network, obviating concentration and control by a single node. Shared ownership of data imparts transparency and safeguards against interference from external parties, fostering a tamper-proof and secure environment.

C.SECURITY AND PRIVACY

Blockchain's robust security mechanisms hinge on cryptographic functions applied to network nodes. The utilization of the SHA-256 cryptographic algorithm on stored hashes fortifies the integrity of data on the blocks. The acronym SHA denotes Secure Hashing Algorithm, and these cryptographic hashes play a pivotal role in ensuring data integrity. Cryptographic hashes, being one-way functions, generate checksums for digital data, impervious to reverse engineering. This cryptographic fortification positions blockchain as a decentralized and secure platform, rendering it an optimal choice for preserving privacy in various applications.

4. CHALLENGES ENCOUNTERED BY BLOCKCHAIN TECHNOLOGY

A. SCALABILITY AND STORAGE CAPACITY

The storage of data on the blockchain poses a dual challenge, specifically centered around issues of confidentiality and scalability. The transparent nature of blockchain, where data is visible to all participants on the chain, introduces concerns about the confidentiality of sensitive information. In the healthcare domain, where extensive datasets encompassing patient medical history, records, lab results, X-rays, MRI reports, and myriad other documents are stored, the sheer volume of data exerts considerable pressure on the storage capacity of the blockchain. Striking a balance between maintaining data privacy and ensuring scalability becomes a pivotal consideration in leveraging blockchain for healthcare applications.[19]

B. DEFICIENCY IN SOCIAL ADOPTION

The intricate workings of blockchain technology remain comprehensible to a select few, presenting a challenge rooted in a scarcity of widespread understanding. Given the early stages of blockchain development and its continual evolution, the transition from established Electronic Health Record (EHR) systems to blockchain technology demands time and concerted effort. Healthcare institutions, including hospitals, face the intricate task of not only grasping the intricacies of blockchain but also executing a comprehensive overhaul of their existing systems to align with the principles and mechanics of blockchain technology. This necessitates a gradual shift, underscoring the imperative for institutions to navigate and bridge the existing knowledge gap during the assimilation of blockchain within the healthcare infrastructure.

C.CHALLENGES IN STANDARDIZATION

The challenges associated with the standardization of blockchain technology become apparent in its adoption landscape. The lack of universally agreed-upon practices for essential components such as smart contracts, data storage methods, and communication protocols creates hurdles, impeding the smooth development of cohesive and interoperable blockchain solutions by developers and organizations.[20]

IV. PRELIMINARIES

This section formally outlines the foundational elements integral to the proposed framework, shedding light on the chosen software platform and its inherent advantages. Furthermore, it delves into the significance of Ethereum and IPFS, the key components crucial for the effective implementation of the framework.

A. ETHEREUM

Ethereum stands as a distributed blockchain network, building upon the foundational concepts of blockchain pioneered by the popular cryptocurrency Bitcoin.[10] Introduced formally in 2015, Ethereum aims to establish a trustless smart contract platform, offering open-source functionality with a programmable blockchain feature. Embracing a peer-to-peer networking structure[21], Ethereum utilizes its cryptocurrency called Ethers, facilitating transactions and interactions among accounts connected to the Ethereum blockchain. Solidity, a specialized programming language for smart contracts, empowers programmers to customize their blockchain operations, defining the distinctive nature of Ethereum's decentralized capabilities.

B. INFORMATION TRANSACTION

Within the Ethereum framework, a transaction acts as the conduit through which external entities interact with the network. This interaction allows external users to update the state of records or information stored on the Ethereum blockchain. [22]Key elements within an Ethereum transaction include the sender's address (From), recipient's address (To), the transferred fund amount in wei (Value), an optional data field for messages sent to the recipient, and Gas – a fee paid by the sender for the transaction operation. Gas comprises Gas Price (the fee the sender is willing to pay) and Gas Limit (the maximum gas paid for the transaction).

C. SMART CONTRACTS

Smart contracts serve as executable code snippets facilitating various tasks on the blockchain. These contracts run directly on the blockchain, ensuring their security against tampering or alterations. Programmed using the Solidity language, smart contracts[23] undergo compilation into EVM bytecode. JavaScript and Python languages, encapsulated within the Solidity framework, provide flexibility for programmers to articulate blockchain operations. After compilation, smart contracts are executed and deployed on the Ethereum[13], [24] blockchain, underscoring their pivotal role in enabling programmable operations.

D. INTERPLANETARY FILE SYSTEM (IPFS)

IPFS, functioning as a protocol employing peer-to-peer networks for data storage, emerges as a secure and tamper-resistant solution. Data stored on IPFS is safeguarded against alterations through cryptographic identifiers, ensuring the integrity of the stored information. Each file on IPFS is assigned a unique cryptographic hash, disallowing duplicate files within the network.[24] The decentralized and secure storage strategy of IPFS makes it an optimal choice for housing critical and sensitive data, reducing computational burdens over the blockchain. Operating on a peer-to-peer network, IPFS utilizes IPFS [25]objects containing unstructured binary data and link arrays. This protocol uniquely identifies files through cryptographic hashes, establishing a robust foundation for secure and decentralized data storage within the proposed framework.

E. DJANGO

Django is a high-level web framework written in Python, designed to promote rapid development and clean, pragmatic design in web applications. Developed to follow the model-view-controller (MVC) architectural pattern, Django simplifies the creation of complex, database-driven websites by providing a robust and flexible foundation. Furthermore, Django incorporates a templating engine that allows developers to create

dynamic and content-rich web pages. The framework's extensive documentation and a vibrant community contribute to its accessibility, making it a preferred choice for both beginners and experienced developers alike. Its adherence to best practices in security makes it a reliable option for building robust and secure web applications. In summary, Django stands as a versatile and powerful web framework that prioritizes efficiency, maintainability, and security, making it an excellent choice for developing a wide range of web applications.

V. SYSTEM DESIGN AND ARCHITECTURE

System design is the most important and vital part of any framework as it is used for the development of the system from its theory. This section includes the modules, architecture and various elements that are combined together to form the whole system’s framework. As defined earlier the purpose behind this proposed framework is to create such a decentralized system that is temper-proof, secure and confidential blockchain-based system for electronic health records. The proposed framework or system has three entities or modules. These modules when combined together would keep our system working. These entities or modules have further concepts that need to be understood they are explained as follows.

The proposed framework consists of users that could be patients, doctors, administration and nursing staff. They were given granular access as they should have varying level of authority on the system.

1.USER LAYER

In the realm of system dynamics, a user stands as an integral entity defined by their adept utilization of the system and its array of resources. Endowed with diverse roles and distinct features within the system, a user becomes an identifiable entity, contributing to the system's functionality.[26] This user layer is composed of individuals with varying roles, encompassing patients, doctors, administrative etc. Within this layer, users undertake the fundamental responsibility of engaging with the system, executing essential tasks that include creating, reading, updating, and deleting medical records. These tasks collectively form the cornerstone of user interactions, emphasizing the user layer's pivotal role in shaping the operational landscape of the system.

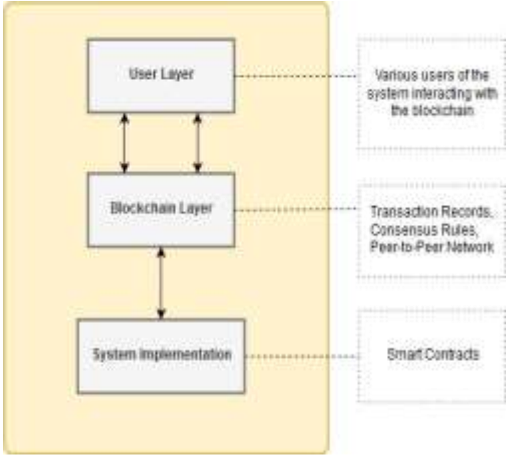
User Layer
Various users of the system interacting with the blockchain
Blockchain Layer
Transaction Records, Consensus Rules, Peer-to-Peer Network
System Implementation
Smart Contracts

Fig3. System design of proposed framework.

2.BLOCKCHAIN LAYER

The succeeding stratum within the system architecture is the blockchain layer, housing the functional code that operates on the blockchain. This layer encompasses three crucial elements, each contributing to the core functionalities of the blockchain:

• Blockchain Assets: Within the Ethereum blockchain, the transaction process emerges as a pivotal mechanism through which external users can modify the state of records or information stored on the Ethereum blockchain network. These transactions assume the role of assets within the Ethereum blockchain, representing pieces of information that users can transmit to one another or store for future use.

• Governance Rules: The broader domain of blockchain technology adheres to consensus rules governing the execution and computation of transactions. To uphold the tamper-proof and secure nature of the blockchain, consensus algorithms are instrumental. Ethereum's blockchain, for instance, employs the Proof of Work (PoW) consensus algorithm, ensuring that governance over the blockchain remains trustworthy and is collectively validated by all trusted nodes connected to the network.

• Network: Ethereum's blockchain layer relies on a peer-to-peer network structure. In this decentralized network, all nodes function as peers, with no single node assuming central control over the network's operations. This design choice emphasizes the creation of a distributed platform rather than a centralized one. The use of a network where all connected nodes possess equal status and rights aligns with the foundational principles of decentralization, enhancing the reliability and security of the technology.

TRANSACTION

The operational transactions embedded within the system encompass a series of functionalities designed to manage and interact with patient medical records in the Decentralized Application (DApp). These transactions include:

•Add Records: This transaction initiates the creation of a patient's medical records within the DApp. The fields of ID, name, co-morbid conditions, blood group, and an IPFS hash are included. The patient's fundamental medical information is stored alongside the IPFS hash, which contains uploaded files like lab results or additional medical records.

• Update Records: Tailored to modify a patient's medical records, this transaction focuses on altering basic patient information while maintaining the non-updateable nature of the IPFS hash. This security measure ensures the integrity and confidentiality of patient records.

• View Records: Enabling users, including both doctors and patients, to access and review medical records stored in the DApp. Patient authentication is implemented to ensure that individuals only view their own records. The system utilizes the patient's public account address to restrict access, guaranteeing that only relevant medical records are accessible.

• Delete Records: This transaction empowers authorized users, specifically doctors, with the ability to delete the records of any patient stored on the blockchain. This right is granted to doctors to facilitate efficient record management.

To regulate access to these transactions, certain users are designated with specific rights. For instance, only doctors and nursing staff possess the authority to make changes to or add patient records. The accessibility to add and update records is restricted to these entities. Additionally, while patients can view their medical records, they are not granted the access to add or update them, reinforcing a controlled and secure access model within the system.

3.SYSTEM IMPLEMENTATION

Reiterating details from preceding sections, the system's realization involved the utilization of Ethereum and its associated dependencies. This section delves deeper into the intricacies of system implementation to provide a comprehensive understanding of the various functions it encompasses.

Ganache
connect Ganache to Metamask
(IMPORT ACCOUNT FROM GANACHE)

Figure 4. Connect Ganache to Metamask

The diagram shows you how to connect Ganache, a local blockchain simulator, to MetaMask, a popular cryptocurrency wallet. Ganache is like a small, private world where you can test and develop your blockchain applications without having to worry about affecting the real Ethereum network. MetaMask is like a passport that lets you interact with the real Ethereum network.

4.SMART CONTRACTS

As elucidated earlier, smart contracts constitute a pivotal component of blockchain technology, serving as the conduits for fundamental operations. The framework incorporates the following contracts to orchestrate various functionalities:

• Patient Records:This contract plays a central role in providing access to users on the blockchain and executing Create, Read, Update, and Delete (CRUD) operations on patient records. Specifically tailored for the proposed framework, the Patient Records smart contract is instrumental in implementing the outlined functionalities.• Roles:The Roles contract assumes a crucial role in defining and allocating distinct roles to users within the system. This contract establishes the necessary permissions and authorizations, ensuring a structured and secure access model for different entities interacting with the blockchain.These contracts collectively contribute to the operational dynamics of the proposed framework, enabling the secure management of patient records and the delineation of roles and permissions for users. The implementation of these smart contracts serves as the backbone for the decentralized system's functionality.

THE PATIENT RECORDS SMART CONTRACT ALGORITHM

Outlined below is the algorithm encapsulating the definition of the Patient Records smart contract. This algorithm meticulously delineates each operation performed within the contract and outlines the various conditions associated with them. It provides a comprehensive insight into how roles are maintained within the contract to grant access to specific functionalities.

The Patient Records smart contract algorithm not only encompasses the CRUD operations performed on patient records but also intricately details the conditions that govern these operations. Furthermore, it offers transparency into the mechanism through which roles are upheld, ensuring a granular and secure access framework for distinct functionalities within the decentralized system.This algorithm serves as a foundational blueprint for the Patient Records smart contract, elucidating the systematic execution of operations and the underlying conditions that safeguard the integrity and security of patient records within the proposed framework.

A. USAGE SCENARIO FOR ALGORITHM 1

Algorithm 1 provides a comprehensive understanding of the smart contract functionality for patient records, delineating five key functions tailored for administrators and other system users. The initial function, define roles, is designated for the administrator. It involves two variables, namely new role and new account, utilized for appending new roles and accounts to the role mapping list. This list serves as a crucial reference for accessing user roles within the system.[26]

The second function, add patient record, is executed by doctors who have been assigned the corresponding role by the administrator in the define roles function. Authentication is enforced by verifying that the operation is carried out by the authenticated public address of the doctor's account, preventing unauthorized access. The use of 'msg.sender' in the Solidity language uniquely identifies the user's address. Once authenticated, doctors can add patient records, concluding the function by saving the updated record.

The third function, "view patient records," requires the passage of the patient ID as a variable. This ID serves as a reference for the system to retrieve and return the patient's records to the requesting account. Role validation is embedded within this function, restricting access to only patients and doctors authorized to view the records.The fourth function, "update patient records," facilitates modifications to the saved records of a patient. A validation process is reiterated to ensure that only authenticated users access this function, maintaining the integrity of the records.

The final function, "delete patient records," explicitly signifies its purpose—to delete the records of a specific patient. Requiring the patient's unique ID as input, this function undergoes a validation process to confirm that the authenticated user, in this case, a doctor, is performing the deletion. This role-based access mechanism guarantees that third parties are barred from accessing these functions, ensuring exclusive access for authenticated system users.

```
Algorithm 1 Smart Contract for Patient Records
Assign Roles:
function Define Roles (New Role, New Account ) add new role and account in roles mapping
end function
Add Data:
function Add Patient Record ( contains variables to add data)
    if ( msg.sender == doctor ) then add data to particular patient’s record
    else Abort session
    end if
end function
Retrieve Data:
functionView Patient Record ( patient id )
    if ( msg.sender == doctor || patient) then
        if ( patient id) == true then retrieve data from specified patient ( id ) return (patient record) to the account that requested the retrieve operation
        else Abort session
        end if
    end if
end function
Update Data:
function Update Patient Record ( contains variables to update data)
    if ( msg.sender == doctor ) then
        if( id == patient id && name == patient name ) then update data to particular patient’s record
            return success
        else return fail
        end if
    else Abort session
    end if
end function

Delete Data:
function Delete Patient Record ( patient id )
    if (msg.sender == doctor ) then
        if ( id == patient id ) then
            delete particular patient’s record
            return success
        else return fail
        end if
    else Abort session
    end if
```

end function

B. WORKING EXAMPLE FOR PROPOSED FRAMEWORK

In the preceding section, it was elucidated that Ethereum served as the implementation platform, and the anticipated block time for Ethereum falls within the range of 10 to 19 seconds. Block time, in this context, denotes the duration required for a new block to be generated within the blockchain. Specifically, for smart contracts, the confirmation time for a transaction is approximately 38 seconds, contingent upon the gas price specified for that particular transaction. Unlike Bitcoin, Ethereum operates without a block size limit, relying instead on a gas limit—a concept elaborated in prior sections.

To delve into the specifics, the time taken for the append function within Algorithm 1, i.e., the "Add Patient Record" operation, is estimated to be around 1 to 2 minutes. This timeframe is contingent upon the size of the data being processed. As for retrieval functions, such as the "View Patient Record" operation in Algorithm 1, the expected duration is approximately 50 seconds.

In essence, these timeframes offer insights into the operational efficiency and speed of the proposed framework, with transaction confirmation times and data processing durations providing valuable benchmarks for evaluating the system's performance under Ethereum's dynamic block time parameters.

C.USAGE SCENARIO FOR PROPOSED FRAMEWORK

The proposed framework unfolds its fundamental usage scenario, centered around two primary entities: the Administrator and the User. The User category is further dichotomized into doctors and patients, both of whom are bestowed with specific roles assigned by the system's administrator—an individual typically hailing from the administrative staff of the hospital. The crux of the administrator's role lies in defining granular access for the two main users, namely doctors and patients.

Commencing the operational sequence, the administrator initiates the activity by assigning roles. This assignment involves specifying both the Role Name and Account Address of the user being endowed with a particular role. Every user within this proposed system possesses a distinct role name and account address integral to their system interaction. Once roles are designated, the administrator records this information in a roles list, serving as a validation repository for subsequent steps.

Following the role assignments, when a user seeks to execute operations within the proposed system, they initiate a request for action. The system meticulously verifies the user's role name and account address against the Roles List, granting access to perform the specified functions upon successful validation. Subsequent to the execution of functions, the system securely archives the pertinent information on the Ethereum Blockchain. This blockchain, functioning as the transactional backbone, ensures the immutable and transparent storage of system data.

VI. PERFORMANCE

In this segment, we delve into an in-depth assessment of the performance metrics associated with our proposed blockchain framework tailored for electronic health records (EHRs). This rigorous evaluation aims to demystify the intricacies of this avant-garde technology, ensuring comprehensibility and elucidating its potential benefits and limitations.

A. EXPERIMENTAL CONFIGURATION

To rigorously evaluate the performance metrics of our innovative framework, a series of experiments were meticulously orchestrated utilizing the following hardware specifications:

- Processor: Intel Core i7-6498DU CPU @ 2.50GHz, augmented by a 2.60 GHz turbo boost capability.

- System Memory: A robust 8.00 GB RAM configuration.

- Operating System: Windows 10 (64-bit) edition, ensuring compatibility and stability.

Our framework's foundational architecture is meticulously crafted using Solidity, Ethereum's designated programming language. Notably, Solidity encapsulates the capabilities of JavaScript and Python, facilitating seamless integration and sophisticated smart contract development within the Ethereum ecosystem.

B. DATA COLLECTION AND METRICS DEFINITION

This section elucidates the comprehensive dataset harnessed for performance evaluation, accompanied by an in-depth exposition of the evaluation metrics employed to ascertain the framework's efficacy and efficiency.

1) TRANSACTIONAL DATA

The evaluation framework leverages specific transactional metrics to discern performance nuances, encompassing:

- Smart Contract Deployment Timestamp (tx1): This metric encapsulates the precise moment when a smart contract undergoes deployment within the Ethereum blockchain network, serving as a pivotal benchmark.

- Transaction Finalization Timestamp (tx2): This crucial metric delineates the temporal dimension associated with transaction completion and subsequent confirmation within the Ethereum ecosystem.

2) PERFORMANCE METRICS EXPLANATION

A trifecta of performance metrics is judiciously employed to quantify and elucidate the framework's operational efficiency and efficacy:

• Execution Duration: This metric quantifies the temporal gap, expressed in seconds, between transaction confirmation and its subsequent execution within the blockchain network. Mathematically articulated as the difference between the maximum (tx2) and minimum (tx1) timestamps.

• Throughput Analysis: This pivotal metric elucidates the volumetric capacity of data transference between disparate locations within a predefined temporal window, offering insights into the framework's data processing capabilities.

• Latency Assessment: This metric encapsulates the temporal delay incurred when system components await requisite responses from interconnected subsystems. In temporal terms, it is quantified as the temporal delta between transaction deployment and finalization timestamps, offering nuanced insights into transactional efficiency and system responsiveness.By meticulously evaluating these performance metrics, the research endeavors to offer empirical insights into the framework's operational capabilities, potential scalability constraints, and avenues for future optimization, ensuring its viability and resilience within evolving healthcare ecosystems.

C. RESULTS

1) PERFORMANCE EVALUATION

To glean actionable insights into the real-world applicability and operational efficiency of our proposed framework, we embarked on a comprehensive performance assessment leveraging Apache JMeter version 5.1.1 coupled with Apache Version 2.00. Apache JMeter stands as a quintessential desktop performance testing instrument, adeptly facilitating the meticulous analysis and evaluation of application functionalities.

a: AVERAGE EXECUTION DURATION

Empirical observations elucidate a proportional relationship between transaction volume and execution time, delineating variances across distinct functional modules encapsulated within the smart contract architecture expounded in Section V. For a singular user engagement scenario, pivotal functions like Assign Roles, Add Patient Records, and View Patient Records manifested respective execution durations of 18.29 seconds, 1 minute 48 seconds, and 50 seconds. However, the temporal benchmarks exhibit discernible escalation in scenarios characterized by concurrent engagements from 100 users, underscoring scalability considerations and transactional throughput dynamics.

b: THROUGHPUT ANALYSIS

Algorithmic elucidation within Section V demystifies the multifarious functions integrated within the smart contract framework. Leveraging JMeter, we orchestrated simulations ranging from 100 to 500 concurrent users, with corresponding throughput representations delineated in KB/sec units. Notably, empirical evaluations underscore a linear correlation between user volume augmentation and throughput amplification, corroborating the framework's intrinsic efficiency and scalability nuances.[26]

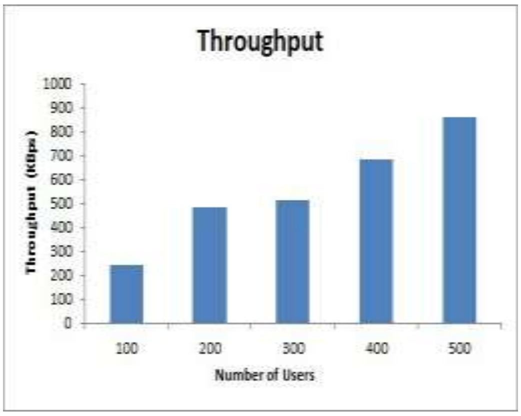

FIGURE 5. Throughput of the proposed framework.

c: AVERAGE LATENCY ASSESSMENT

Latency, as previously articulated, encapsulates the temporal delta between transaction initiation and requisite system responses, offering poignant insights into operational responsiveness and system efficiency. Methodologically, JMeter serves as the instrumental conduit for latency quantification, wherein simulations spanning diverse user volumes enable meticulous latency evaluations calibrated in milliseconds. Figure 5 provides an illustrative encapsulation of the system's average latency metrics juxtaposed against throughput dynamics. Remarkably, empirical analyses demarcate the pinnacle latency threshold at a mere 14 milliseconds, accentuating the framework's optimized responsiveness and transactional efficiency.

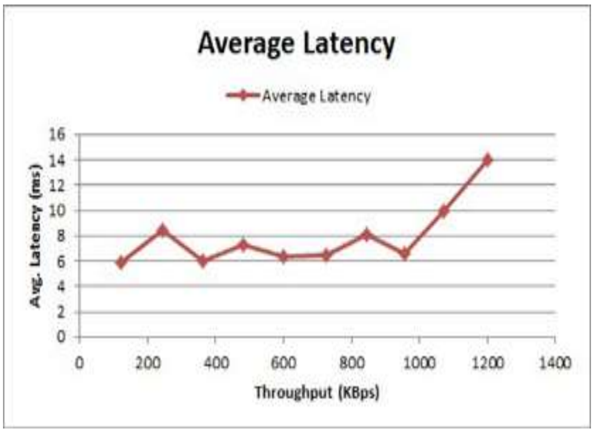

FIGURE 6. Average Latency of the proposed framework.

By meticulously dissecting these performance metrics, the research endeavors to proffer empirical validations, facilitate stakeholder engagement, and engender iterative refinements, ensuring the proposed framework's sustained viability, scalability, and resilience within the burgeoning landscape of healthcare data management and electronic health record (EHR) safeguarding paradigms.

2) EVALUATION OF TRANSACTIONAL PERFORMANCE

Our assessment delves into the efficacy of the proposed framework, concentrating on transactional dimensions encompassing size and economic implications. Prior to a comprehensive evaluation of transaction sizes, a nuanced analysis of transaction payload becomes imperative. This examination unfolds in subsequent sections.Every Ethereum transaction embeds a data payload, instrumental in triggering smart contract functionalities. This payload adopts a hex-serialized format, intricately intertwined with bytes. For elucidation purposes, we pivot towards dissecting two pivotal functions encapsulated within Algorithm 1, aiming to decipher the underlying transactional payload intricacies.Within this Ethereum transactional paradigm, the data payload emerges as a pivotal yet optional facet, exclusively activated during engagements with contract functionalities. This payload bifurcates into:

- Function Selector
- Function Arguments

The function selector, derived as the initial 4 bytes of a Keccak-256 hash, serves as a quintessential identifier, pinpointing the invoked smart contract function. Concurrently, function arguments encapsulate a myriad of static and dynamic elements, each necessitating distinctive encoding modalities within the payload realm.

To demystify this, let's dissect the 'Define Roles' function from Algorithm 1. The ensuing Keccak-256 hash, when scrutinized, unravels the function selector—essentially the function's signature. For illustrative purposes, consider the function signature as: Define Roles (string, address). Notably, this function's encoding culminates in a 64-byte payload representation, encapsulating both static and dynamic parameter nuances.Such analytical endeavors pave the way for comprehensive payload matrices, spanning the functional spectrum delineated within Algorithm 1. Table 2 offers an exhaustive compendium of these payloads, facilitating stakeholders' transactional analytics endeavors.Transitioning from payload nuances, Table 3 meticulously catalogues transaction sizes in byte metrics, anchoring perspectives within Algorithm 1's functional array. It's imperative to note that this section's transactional dimensions emanate from a payload-centric vantage, diverging from Section V's block size-centric assessments.Furthering our exploration, Ethereum's intricate fee dynamics necessitate scrutiny, denominated in 'ETH' with ancillary units such as wei and gwei. The ensuing formula crystallizes transactional cost determinants:[26]

Transaction Fee = gasConsumed × gasPrice

Leveraging recommended parameters, namely 21,000 for gas consumption and 21 Gwei for gas price, we derive:

Transaction Fee = 21,000 × 21 = 441,000 Gwei

Translating this to Ethereum metrics, 1 Ether equates to 1,000,000,000 Gwei, rendering the transaction fee for 1 Ether as 0.00041 Gwei, as encapsulated in Table 3's transactional fee matrix.

3) FRAMEWORK BENCHMARKING AGAINST CONTEMPORARY RESEARCH

Our discourse extends to benchmarking pivotal parameters inherent to our framework against contemporaneous research trajectories within this domain. While ensuring parameter inclusivity, paramount emphasis converges on safeguarding system sanctity, meticulously balancing security and privacy paradigms.[22] Each parameter, juxtaposed against related works, undergoes rigorous scrutiny, ensuring congruence with overarching security and privacy mandates.

4)COMPARISON OF PROPOSED FRAMEWORK WITH RELATED WORK

In evaluating our framework against existing works in this domain, several parameters are scrutinized to ensure their presence in our framework while maintaining the utmost security and privacy. The discussion of each parameter is accompanied by an exploration of its impact on the overall security and privacy of the system.

A. SCALABILITY

Scalability, in the context of information systems, gauges the system's proficiency in handling varying storage volumes. Blockchain technology grapples with scalability concerns, and our proposed system addresses this issue by incorporating an off-chain storage mechanism. Patient data, stored on the blockchain, includes basic information alongside an IPFS hash—an off-chain scaling solution. This strategic approach not only resolves scalability challenges but also accelerates transaction processing. The cryptographic hash utilization in IPFS, managed via a decentralized peer-to-peer network, ensures that scalability enhancements do not compromise the system's security.

B. INTEGRITY

Integrity in a system is contingent on its trustworthiness and resistance to tampering. The blockchain-based system upholds the integrity criterion steadfastly. Information stored within the system remains unaltered and impervious to unauthorized modifications. Exclusive access is granted solely to associated parties, namely doctors and patients, while users and third parties lack the privilege to make alterations to the smart contract. Access rules further fortify the security, ensuring the temper-proof nature of patients' medical records. Additionally, the utilization of IPFS for record storage bolsters the security of patients' medical data.

C. ACCESS CONTROL

The framework employs a robust Role-based access mechanism to mandate that every entity within the system is assigned a specific role. Unauthorized third parties are systematically barred from accessing the system. The dual-layered security is underpinned by the inherent security protocols of blockchain technology and the stringent access control enforced by the Role-based mechanism. This approach not only guarantees the security of patient records but also assures that access is exclusively granted to duly authorized system users. This parameter reinforces the safeguarding of patients' personal medical data, ensuring that only authorized entities have access to the system and its functionalities.

D.CONTENT-ADDRESSABLE STORAGE

The content-addressable storage in our proposed framework leverages IPFS as its off-chain storage mechanism [20]. Patient records, being sensitive in nature, are securely stored on IPFS, generating a hash for each stored record. This hash is subsequently stored on the blockchain, serving as a reference point for retrieval by doctors and patients as needed. The cryptographic hashing mechanism employed by IPFS guarantees the security of the stored data, reinforcing the overall security of our proposed framework. This content-addressable storage approach provides an additional layer of protection, ensuring the integrity and confidentiality of patient records within the system.

VII.CONCLUSION AND FUTURE WORK

This paper extensively explored the applicability of blockchain technology in the healthcare sector, specifically focusing on its potential for enhancing electronic health records (EHR) systems. Despite notable advancements in healthcare and EHR technologies, persisting challenges prompted the exploration of blockchain as a novel solution. The proposed framework amalgamates secure record storage with finely tuned granular access rules, creating a user-friendly system. The utilization of off-chain storage via IPFS addresses data storage concerns, while role-based access ensures that medical records remain accessible only to trusted individuals, mitigating information asymmetry within EHR systems.Looking ahead, our future work involves the implementation of a payment module within the existing framework. This endeavor requires careful consideration, including decisions on the appropriate fees for patient-doctor consultations within a decentralized blockchain system. Additionally, defining policies and rules that align with healthcare sector principles will be crucial for the successful integration of the payment module. This expansion aims to further enhance the functionality and practicality of the proposed framework in real-world healthcare scenarios.

REFERENCES

[1] G. Jetley and H. Zhang, “Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,”’ Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019.,” vol. 126, pp. 113–-137, Nov. 2019.

[2] A. L. and C. A. C. K. Wisner, “““The electronic health record’s impact on nurses” cognitive work: An integrative review,’’ Int. J. Nursing Stud.,” vol. 94, p., pp. 74–84, 2019.

[3] M. Hochman, “““Electronic health records: A ‘“Quadruple win,”’ a ‘“quadru- ple failure,”’ or simply time for a reboot?”’ J. Gen. Int. Med.,” vol. 33, pp. 397–399, 2018.

[4] H. H. S. P. S. K. E. K. J. T. A. M. A. and T. H. T. Vehko, “‘‘Experienced time pressure and stress: Electronic health records usability and information technology compe- tence play a role",” BMC Med. Inform. Decis., vol. 19, pp. 1–160, 2019.

[5] M. Reisman, “‘‘EHRs: The challenge of making electronic data usable and interoperable.,” vol. 42, pp. 572–575, 2017.

[6] M. M. D. S. A. W.-D. and M. W.-S. W. W. Koczkodaj, “““Electronic health record breaches as social indica- tors,”’ Social Indicators Res,” vol. 141, p. . 861-–871, 2019.

[7] N. E. B. B. E.-C. and A. F. S. T. Argaw, “‘‘The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,’” vol. 19, pp. 1–10, 2019.

[8] A. McLeod and D. Dolezel, “““Cyber-analytics: Modeling factors associated with healthcare data breaches,”’ ,” vol. 108, pp. 57-–68, 2018.

[9] O. K. N. B. and T. D. D. Spatar, “““Adoption factors of electronic health record systems,”’ Technol.,” vol. vol.58, 2019.

[10] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electrnic Cash System,” 2008.

[11] W. J. Gordon and C. Catalini, “““Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,”’ Comput. Struct. Biotechnol. J,” vol. vol.16, pp. 224-–230, 2018.

[12] J. Eberhardt and S. Tai, “‘‘On or off the blockchain? Insights on off-chaining computation and data,” pp. 11–45, 2014.

[13] D. J. and S. R. D. Vujičić, “ ‘‘Blockchain technology, bitcoin, and Ethereum: A brief overview,’” pp. 1–6, 2018.

[14] Y. Y. X. W. J. L. R. Q. and F.-Y. W. S. Wang, “‘‘An overview of smart contract: Architecture, applications, and future trends,’” pp. 108–113, 2018.

[15] H.-E. K. and L. O.-M. T.-T. Kuo, “‘‘Blockchain distributed ledger technologies for biomedical and health care applications,” vol. 24, no. 2017.

[16] ‘‘HBasechainDB M. S. Sahoo and P. K. Baruah, “A scalable blockchain framework on Hadoop ecosystem,’’ in Supercomputing Frontiers,” pp. 18–29, 2018.

[17] J. W. D. C. S. G. L. and S. T. R. P. Zhang, “““FHIRChain: Applying blockchain to securely and scalably share clinical data,”’” pp. 2767–2769, 2018.

[18] S. X. H. D. X. C. and H. W. Z. Zheng, “““An overview of blockchain technology: Architecture, consensus, and future trends,”’” pp. 557–564, 2017.

[19] C. Pirtle and J. Ehrenfeld, “““Blockchain for healthcare: The next generation of medical records?”’ ,” vol. vol.42, pp. 9–172, 2018.

[20] A. Z. J. M. Z. K. A. A. K. and G. S. A. A. Siyal, : “Challenges and future perspectives,” vol. vol.3, pp. 1–3, 2019.

[21] S. Gupta and M. Sadoghi, “““Blockchain transaction processing,”’ in Encyclopedia of Big Data Technologies.,” pp. 366–376, 2019.

[22] G wood, “‘‘Ethereum: A Secure Decentralised generalised transaction ledger.,” 2017.

[23] M. B. T. C. S. L. and R. Z. N. Atzei, “““SoK: Unraveling bitcoin smart contracts,”’ in Proc. Int. Conf. Princ. Secur. Trust, Thessaloniki, ,” pp. 217–242, 2018.

[24] S. J. S. S. and N. K. T. Dey, “““HealthSense: A medical use case of Internet of Things and blockchain,”’” pp. 486–491, 2017.

[25] “InterPlanatery File System (IPFS).,” http://ipfs.io/., 2019.

[26] U. Q. A. A. K. AYESHA SHAHNAZ 1, “Using blockchain for Electronic Health Records,” 2019.