Using Blockchain for Electronic Health Records

AYESHA SHAHNAZ[ID]1, **USMAN QAMAR**1, **AND AYESHA KHALID**[ID]2, **(Member, IEEE)**

1Computer Science Department, National University of Science and Technology (NUST), Islamabad 44000, Pakistan
2The Centre for Secure Information Technologies (CSIT), ECIT Institute, Queen's University of Belfast, Belfast BT7 1NN, U.K.

Corresponding author: Ayesha Shahnaz (aisha.shehnaz@gmail.com)

ABSTRACT Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management. In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework. Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chain storage of the records. This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain-based solution.

INDEX TERMS Blockchain, health records, electronic health records, decentralization, and scalability.

I. INTRODUCTION

The recent advent in technology is affecting all parts of human life and is changing the way we use and perceive things previously. Just like the changes technology has offered in various other sectors of life, it is also finding new ways for improvement in healthcare sector. The main benefits that advancement in technology is offering are to improve security, user experience and other aspects of healthcare sector. These benefits were offered by Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems. However, they still face some issues regarding the security of medical records, user ownership of data, data integrity etc. The solution to these issues could be the use of a novel technology, i.e., Blockchain. This technology offers to provide a secure, temper-proof platform for storing medical records and other healthcare related information.

Before the advent of modern technology, healthcare sector used paper based system to store the medical records, i.e., using handwritten mechanism. This paper-based medical record system was inefficient, insecure, unorganized and was not temper-proof. It also faced the issue of data- duplication

and redundancy as all the institutions that patient visited had various copies of patient's medical records.

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 safety aspect of the patients by preventing errors and increasing information access [2]. The goal of EHR systems was to solve the problems faced by the paper-based healthcare records and to provide an efficient system that would transform the state of healthcare sector [3].

The EHR systems have been implemented in a number of hospitals around the world due the benefits it provides, mainly the improvement in security and its cost-effectiveness. They are considered a vital part of healthcare sector as it provides much functionality to the healthcare [4]. These functionalities are electronic storage of medical records, patients' appointment management, billing and accounts, and lab tests. They are available in many of the EHR system being used in the healthcare sector. The basic focus is to provide secure, temper-proof, and shareable medical records across different platforms. Despite the fact that notion behind usage of EHR systems in the hospitals or healthcare was to improve the quality of healthcare, these systems faced certain problems

The associate editor coordinating the review of this manuscript and approving it for publication was Kim-Kwang Raymond Choo[ID].

and didn't meet the expectations associated with them [3]. A study was conducted in Finland to find the experiences of nursing staff with the EHR, it was concluded that EHR systems faced the problems related to them being unreliable and having a poor state of user-friendliness [5]. The EHR system also faces some other problems which are as follows:

A. INTEROPERABILITY

It is the way for different information systems to exchange information between them. The information should be exchangeable and must be usable for further purposes. An important aspect of EHR systems is its Health Information Exchange (HIE) or in general data sharing aspect. With a number of EHR systems being deployed in various hospitals they have a varying level of terminologies, technical and functional capabilities which makes it to have no universally defined standard [6]. Moreover, at technical level the medical records being exchanged should be interpretable, and that interpreted piece of information could be further used [6].

B. INFORMATION ASYMMETRY

Today the greatest problem in healthcare sector defined by the critics is information asymmetry which refers to one party having better access to information than the other party. In case of EHR systems, or in general healthcare sector is suffering from this problem as doctors or hospitals have access to the patient's records, thus making it central. If a patient wants to access his medical records he would have to follow a long and tedious process to access them. The information is centralized to only a single healthcare organization and its control is only provided to the hospitals or organizations.

C. DATA BREACHES

Data breaches in healthcare sector also calls for the need of a better platform. A study [7] was done for analyzing the data breaches in EHR systems and it depicted that 173 million data entries have been compromised in these systems since October 2009. Another study conducted by Argaw *et al.* [8], explains that hospitals have become a target of cyber-attacks and an increasing trend has been witnessed by the researchers while conducting this study that a lot of research work has been done in this domain [9]–[11].

Moreover, many EHR systems are not designed to fulfill the needs and requirements of the patients and face the issues related to inefficiency and poor adaptation of these systems [12]. The literature also suggests that use of EHRs have introduced negative consequences to information processing [2]. These problems make it reasonable to find a platform that would be helpful in transforming healthcare sector to be patient-centered, i.e., Blockchain. A platform which is secure, transparent and it also provides data integrity to the medical records of the patients.

This paper proposes a framework that creates such a decentralized platform that would store patient's medical records and give access of those records to providers or concerned individuals, i.e., patient. We also intend to solve the

scalability problem of blockchain, as it is not in the design of blockchain to store huge volumes of data on it. So, we would use off-chain scaling method that makes use of the underlying medium to solve the scalability problem by storing the data on that medium. Moreover, our proposed work is intending to solve the above mentioned information asymmetry and data breaches problem faced by the EHR system.

This paper is organized as follows the section II of this paper summarizes the basics of blockchain technology and its dependencies; section III narrates the related work done in this domain. The section IV explains the design and architecture of the proposed framework and section V explains the performance of this framework. The last section provides the conclusion and references.

II. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES
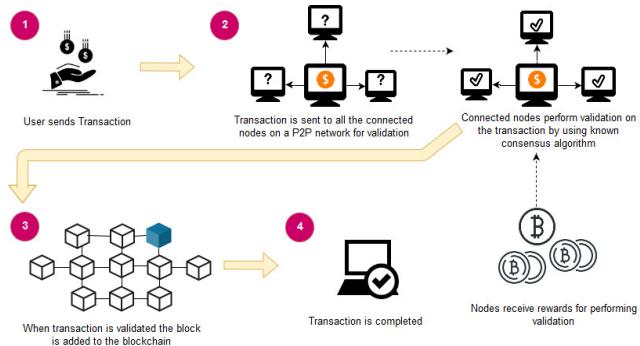
This technology was introduced by Nakamoto [13], for his popular work of digital currency or crypto-currency, i.e., bitcoin. Nakamoto used blockchain technology to solve the double spending problem of bitcoin but soon this novel technology was being used in many other applications.

Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership. Blockchains holds batches of transactions that are hashed thus providing them security and they are managed by peer-to-peer networks. A blockchain has certain benefits such as security, anonymity, and integrity of data with no third party intervention. These benefits make it a reasonable choice to store patient's medical records on it, because the innovation of technology in the healthcare industry has made the security of patient's medical data a top priority. A number of researchers have also identified that using blockchain technology in healthcare would be a feasible solution [14]–[16].

A. ARCHITECTURE

To understand the blockchain architecture let us use the following figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

1. A new transaction being sent by a user on the blockchain network suggests that a new block is created. A block in the blockchain is used for keeping transactions in them and these blocks are distributed to all of the connected nodes in the network. That transaction placed inside a block is broadcasted to all of the nodes in the network. All the nodes in the network have a copy of the complete blockchain that helps them in verification process. When a block containing the user transaction is broadcasted to all of the connected nodes, they verify that the block is not tampered by any means. If this verification results in success then the nodes add that block in their own copy of blockchain.

2. This whole process of the block being added on the blockchain is done by the nodes reaching upon a consensus where they decide which blocks are valid to be added on the blockchain and which are not. This validation is performed by the connected nodes using some known algorithms to verify the transaction and to ensure that sender is an authenticated part of the network. When a node succeeds in performing the validation that node is rewarded with crypto-currency. This process of validating the transaction is known as mining and the node performing this validation is known as miner.
3. After validation is done that block is added to the blockchain.
4. After the whole process of validation is performed the transaction is completed.

Some basic concepts of blockchain technology can be understood in the following descriptions.

B. BLOCK
As explained earlier blockchain are formed together by a number of blocks connected together in a peer-to-peer network thus making a decentralized application. The header of these blocks contains hashes of previous blocks in them. A block contains three things in it which are data, hash of current block and hash of previous block. The data could be anything as it depends on the type of blockchain. As in case of bitcoin, the data consists of coins that are actually electronic cash [13]. The hash that is stored in these blocks contains a SHA-256 cryptographic algorithm which is used for unique identification of a block on the chain.

C. CONSENSUS ALGORITHM
Each block that is added on the chain would need to follow some consensus rules for it to be added on the blockchain. For this purpose blockchain technology uses consensus algorithms. The most common consensus algorithm used is Proof of Work (PoW) algorithm and it was used by Nakamoto [13], in bitcoin network. The basic working of this algorithm is that there are number of nodes or participants on a blockchain network so when a transaction is requested to be

added on the network by any participating node it needs to be calculated. This process is called mining and the nodes that are performing these calculations are miners [17].

D. KEY FEATURES OF BLOCKCHAIN
1) DECENTRALIZATION
With blockchain the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data that was before concentrated at one central point is now handled by many trusted entities.

2) DATA TRANSPARENCY
Achieving data transparency in any technology is to have a trust based relationship between entities. The data or record at stake should be secured and temper proof. Any data being stored on the blockchain is not concentrated at one place and is not controlled by one node but is instead distributed across the network. The ownership of data is now shared and this makes it to be transparent and secure from any third party intervention.

3) SECURITY AND PRIVACY
Blockchain technology uses cryptographic functions to provide security to the nodes connected on its network. It uses SHA-256 cryptographic algorithm on the hashes that are stored on the blocks. SHA stands for *Secure Hashing Algorithm,* these hashes provide security to the blockchain as data integrity is ensured by them. Cryptographic hashes are strong one way functions that generate checksum for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by the cryptographic approaches which makes it to be a good option for privacy protection of certain applications.

E. CHALLENGES FACED BY BLOCKCHAIN TECHNOLOGY
1) SCALABILITY AND STORAGE CAPACITY
Storage of data on the blockchain causes two main problems, i.e., confidentiality and scalability. The data on the blockchain is visible to everyone that is present on the chain this makes the data vulnerable which is not a desired outcome for a decentralized platform. The data stored on the blockchain would contain patient medical history, records, lab results, X-rays reports, MRI results and many other reports, all of this voluminous data is to be stored on the blockchain that would highly affect the storage capacity of blockchain [18].

2) LACK OF SOCIAL SKILLS
The way the blockchain technology works is understandable by very few people. This technology is still in its initial phases and is constantly evolving. Moreover, the shift from trusted EHR systems to the blockchain technology would take time as hospitals, or any other healthcare institutes need to completely shift their systems to blockchain.

TABLE 1. Benefits and barriers of blockchain technology.

Benefits	Decentralized	The data or information stored on the blockchain is distributed across the network
	Data Transparency	Data stored on the blockchain is temper-proof
	Security and Privacy	Blockchain uses cryptographic algorithms to secure any information being stored on it
Barriers	Scalability, Storage Capacity	Storing huge volumes of data on the blockchain would cause storage and scalability problems
	Lack of social skills	As blockchain is an evolving technology and it is not a well understood technology so, it is quite challenging to shift the previously used systems on this technology
	Lack of universally defined standards	There are no defined standards and principles for blockchain technology that are universally applied which makes it difficult to enforce it throughout a specific domain

3) LACK OF UNIVERSALLY DEFINED STANDARDS

As this technology is still in the initial phases and is constantly evolving so there is no defined standard for it. Due to this the implementation of this technology in healthcare sector would also take more time and effort. As it would require certified standards from international authorities that overlook the standardization process of any technology [19]. These universal standards would benefit in deciding upon the data size, data format and type of data that could be stored on the blockchain. Moreover, the adaptation of this technology would become easier due to the defined standards, as they could be easily enforced in the organizations.

III. RELATED WORK

Blockchain technology was designed by Nakamoto [13], the basic idea was to have a cryptographically secured and a decentralized currency that would be helpful for financial transactions. Eventually, this idea of blockchain was being used in various other fields of life; healthcare sector also being one of them intends to use it. A number of researchers have carried out the research on this area, these research works focus on the fact that whether the idea of using blockchain for healthcare sector is feasible or not. They also identify the advantages, threats, problems or challenges associated by the usage of this technology. Some researchers also discussed the challenges that would be faced while actually implementing this on a larger scale.

A. THEORETICAL/ANALYTICAL BLOCKCHAIN-BASED RESEARCH

Gordon and Catalini [14], conducted a study that focused on the methods by which blockchain technology would facilitate the healthcare sector. They identified, that healthcare sector is controlled by hospitals, pharmaceutical companies and other involved third parties. They specified data sharing as the key reason why blockchains should be used in healthcare. This study also identified four factors or approaches due to which healthcare sector needs to transform for usage of blockchain technology. These include way for dealing of digital access rights, data availability, and faster access to clinical records and patient identity. It also discusses the on-chain and off-chain storage of data. The study also included the challenges or barriers faced by usage of blockchain technology these were huge volume of clinical records, security and privacy, patient engagement.

Eberhardt and Tai [20], conducted a study to understand possible approaches to solve the scalability problem of blockchain and also to identify such projects that intend to solve this problem. They define blockchain as composition of various computational and economical concepts based on peer-to-peer system. The aim of this study was to find which data should be stored on-chain and what could be stored off-chain. This study presented five patterns for off-chain storage of data and also includes the basic ideas and implementation framework of these patterns. The authors explain on-chain data is any data that is stored on the blockchain by performing transactions on it. While off-chain data storage is to place data elsewhere on any other storage medium but not on-chain and it also would not include any transactions.

Vujičić *et al.* [21], presented an overview of blockchain technology, bitcoin and Ethereum. The authors define that information technology landscape is constantly changing and blockchain technology is benefiting the information systems. They explained bitcoin as a peer-to-peer distributed network used for performing bitcoin transactions. They also defined that proof-of-work consensus algorithm along with the mining of blockchain concept. The authors emphasize on the fact that scalability is a severe problem faced by blockchain and that certain solutions are proposed for solution of scalability problem these include SegWit and Lightning, Bitcoin Cash and Bitcoin Gold. The paper also explained Ethereum and its dependencies and it also differentiates Ethereum blockchain from bitcoins' blockchain.

Wang *et al.* [22], conducted a study that focused on smart contracts and its application in blockchain technology. They first introduce the smart contracts, their working framework, operating systems and other important concepts attached with them. The authors also discuss that how could smart contracts be used for the new concept of parallel blockchains. They identify that reason of using smart contracts in blockchain is due to the decentralization that is offered through the programming language code written in them. After introducing the basics of smart contract the author explained the various layers of blockchain that combine together to keep system functioning. These layers are data, network, consensus, incentive, contract, and application layer. The paper not only discusses the architecture and framework followed by smart contracts but it also gives an insight on its applications and challenges. The paper also discusses an important future trend

of parallel blockchain that intends to create such blockchain that can optimize two different but important modules.

Kuo *et al.* [23], conducted a review that discussed several applications of blockchain in biomedical and healthcare sector. The authors identified that using blockchains for this domain offers many advantages and some of these are decentralization, persistence of clinical or medical records, data pedigree, and continuous accessibility to data and lastly secure information being accessible to biomedical or healthcare stakeholders. The limitations of blockchain technology were identified to be, confidentiality, speed, scalability and threat of malicious attack, i.e., 51% attack. The authors identified these limitations to be critical for healthcare or biomedical sector as they are being used to store sensitive medical or clinical records. The solution to these problems were presented by authors to store sensitive medical data off-chain, encryption of data to ensure confidentiality, and lastly to use VPNs (Virtual Private Networks) to ensure safety from malicious attacks.

B. PROTOTYPE/IMPLEMENTATION BLOCKCHAIN-BASED RESEARCH

Sahoo and Baruah [24], proposed a scalable framework of blockchain using Hadoop database. In order to solve the scalability problem of blockchain, they proposed to use the scalability provided by the underlying Hadoop database along with the decentralization provided by the blockchain technology. They used the method to store blocks on the Hadoop database, the blockchain on top of this framework includes all of the needed dependencies of blockchain but the blocks are stored on Hadoop database to improve scalability of the blockchain technology. To tackle the scalability problem of blockchain platform this study offers to use Hadoop database system, along with SHA3-256 for hashing used for transactions and blocks. The programming language used for this architecture was Java. This study, was helpful in understanding that blockchain can be used with other platforms that are scalable to improve or solve the scalability of this platform.

Zhang *et al.* [25], proposed a scalable solution to the blockchain for clinical records. The basic aim of this study was to design such an architecture that complies with the Office of National Coordinator for Health Information Technology (ONC) requirements. This study identified the barriers that this technology faces mainly include concerns related to privacy, security of blockchain, and scalability problems related to huge volume of datasets being transmitted on this platform, and lastly there is no universal standard enforced for data being exchanged on blockchain. This study also include a demonstration of a decentralized application (DAPP) based on the design formulated on the ONC requirements as mentioned before. They also included the lessons learnt and how can FHIR chain be improved.

Kim *et al.* [26] proposed a system for management of medical questionnaires and the aim of this system is data sharing through blockchain technology. The authors explain that selection of data storage and sharing of medical questionnaire

is to use this data for further medical and clinical research purposes. They emphasized that it would be helpful for developing diagnosis system, resolving terminologies being used in EHR systems and security issues associated with these systems was also a reason due to which authors selected blockchain technology for their proposed framework. This study contains two main functions, i.e., to create, store the data gathered by questionnaires and to share that data. Another benefit proposed by the system is the validation of the questionnaire being submitted in the system. The questionnaires that are added on this system are first validated to be correct specified format and then are parsed to differentiate the personal data and specific data related to questionnaire results. This would ensure that data could be shared for future research purposes. The authors also address the scenario when a third party requests to access this questionnaire data, this would need the patients' permission that is asked by the doctor to let third party view that data.

IV. PRELIMINARIES

This section formally describes the preliminaries used in proposed framework. It describes the software platform used for development of this framework and its advantages. Ethereum and IPFS being the most prominent and important for implementation of this framework are also discussed in the following section.

A. ETHEREUM

Ethereum is a distributed blockchain network that uses the idea of blockchain that was previously used in the popular crypto currency Bitcoin [13]. Ethereum was formally introduced in year 2015 and the idea behind Ethereum was to create a trustless smart contract platform that would be open-source and would also hold the feature of programmable blockchain. This technology also shares the peer-to-peer networking that makes it distributed. This platform also makes use of its own crypto currency known as *Ethers* [27]. This crypto currency can be used for sharing it between accounts connected on Ethereum blockchain [28]. Ethereum also provides the programmers a language in which they can customize their own blockchain, this language is known as *Solidity*. It was developed for smart contracts that are the main feature of Ethereum.

B. INFORMATION TRANSACTION

In Ethereum, transaction is the way external entity would interact with Ethereum. It can be used by external user to update the state of the record or information stored on the Ethereum blockchain network. An Ethereum transaction contains following elements [29]:

- **From –** message sender, having a 20-bytes address.
- **To –** message recipient, also having a 20-bytes address.
- **Value -** the fund amount (wei) transferred from sender to recipient

- **Data (optional)** – contains the message that is being sent to the recipient
- **Gas** – For every transaction on the Ethereum blockchain the sender needs to pay some fees for performing that operation this fee is known as Gas. Every transaction contains the *gas limit* and *gas price* in it.
  - **Gas Price:** that fee the transaction sender is willing to pay for gas
  - **Gas Limit:** maximum gas that could be paid for this transaction

C. SMART CONTRACTS

Smart contract are known as the piece of code that is used to perform any task on the blockchain. This piece of code is executed when the users send the transactions [30]. They run on the blockchain directly thus making themselves secure from any kind of tampering and alterations. Smart contract commonly use solidity language and they can be used to program any kind of operation that a programmer wants to do on the blockchain. After programming the required operations the programmers can compile them by using EVM bytecode that would be explained in next section. And after compiling them it could be executed and deployed on the Ethereum blockchain [21]. The programming language of JavaScript and Python are encapsulated with the Solidity language provided by Ethereum to write code in smart contracts.

D. ETHEREUM VIRTUAL MACHINE (EVM)

The key benefits that Ethereum platform offers include the programmable blockchain. It provides its users with the choice to create their own applications functioning on the Ethereum. The applications built using this platform are known as *Distributed Applications* (DApps). They contain a number of protocols that are packaged together to create a platform for DApps. These DApps contain smart contracts that have code defined by the user to perform some defined task of an application. That code is deployed and executed using the Ethereum Virtual Machine (EVM) [29], [31]. Thus, the applications that are created using the smart contract are in actual being run on EVM.

E. INTERPLANATERY FILE SYSTEM (IPFS)

IPFS is a protocol that uses peer-to-peer network for data storage. It provides secure data storage as data stored on IPFS is protected from any alteration. It uses a cryptographic identifier that protects the data from alteration as any attempt to make change on the data stored on IPFS could only be done by changing the identifier. All the data files stored on IPFS contains a hash value that is generated cryptographically. It is unique and is used for identification of stored data file on the IPFS [32].

This secure storage strategy of IPFS protocol makes it a favorable choice for storing critical and sensitive data. The cryptographic hash that is generated could be stored on the

decentralized application to reduce the exhaustive computational operations over the blockchain.

IPFS protocol works using a peer-to-peer (P2P) network, this network contains a data structure known as IPFS object that contains data and link in it. Data is unstructured binary data and link consists of an array. The IPFS protocol works in the following way [33]:

- Files stored on IPFS are assigned a unique cryptographic hash
- Duplicate files are not allowed to exist on the IPFS network
- A node on the network stores content and index information of the node

V. SYSTEM DESIGN AND ARCHITECTURE

The related work section includes the work done in the domain of health care being implemented using blockchain technology. As mentioned they provided certain solutions for solving the prevalent problems in blockchain technology. The studies in discussion were mainly addressing the problems of scalability and data sharing through blockchain. They propose the solution of using an underlying database, pertaining to some ONC requirements and any other defined standards to solve them. In contrast to those solutions our proposed framework offers to solve this problem of scalability by using off-chain scaling mechanism of IPFS. Moreover, Ethereum is used for the overall implementation of the proposed framework. Ethereum and its dependencies are also discussed in the previous sections of this paper.

A. SYSTEM DESIGN
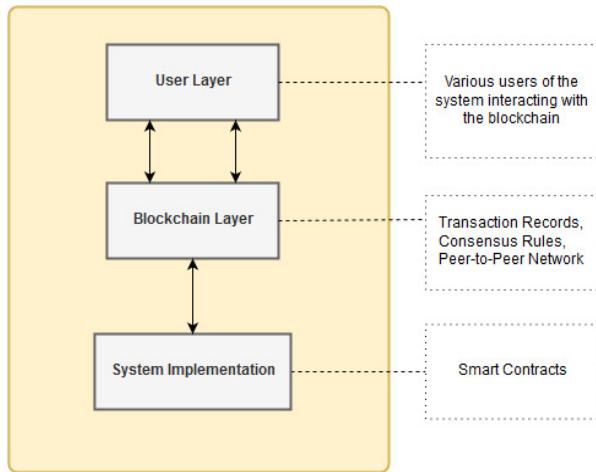
System design is the most important and vital part of any framework as it is used for the development of the system from its theory. This section includes the modules, architecture and various elements that are combined together to form the whole system's framework. As defined earlier the purpose behind this proposed framework is to create such a decentralized system that is temper-proof, secure and confidential blockchain-based system for electronic health records.

As visible in below figure 2, 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

A user of a system is defined as an individual who makes effective use of the system and its resources. A user has various roles and features on the system, making him identifiable on the system.

FIGURE 2. System design of proposed framework.

The users of this system could be patients, doctors and administrative staff etc. The main task of these users would be to interact with the system and perform basic tasks such as create, read, update and delete the medical records. The users using this system would be accessing the system's functionality by a browser which in technical terms we refer as DApp browser, as it is containing the GUI (Graphical User Interface) of the DApp, i.e., our proposed system framework. The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

2) BLOCKCHAIN LAYER

The next layer on the system is the blockchain layer; this layer contains the code or mechanism for interaction of user with the DApp which is functioning on the blockchain. This layer contains three elements inside it. They are:

- **Blockchain Assets:** In Ethereum blockchain, transaction is the process by which external user can update the state of the record or information stored on the Ethereum blockchain network. These transactions are treated as *assets* by the Ethereum blockchain as they are piece of information that user can send to another user or to simply store it for using it later.
- **Governance Rules:** Blockchain technology in general follows some consensus rules for its transactions to be done and computed. For this purpose it needs some consensus algorithms to keep the blockchain temper-proof and secure. Ethereum blockchain uses Proof of Work (PoW) consensus algorithm, the reason behind using it is also for ensuring that *governance* of blockchain is maintained in a trusted manner which is through consent from all the trusted nodes attached to the blockchain network.
- **Network:** Ethereum blockchain uses the peer-to-peer network. In this network all the nodes are connected as

peers. With no node acting as the central node controlling all the functions of the network. The reason behind using this network was because the idea was to create a distributed platform not a centralized. So, using a network where all the connected nodes have equal status and right was the best choice this technology could have done.

TRANSACTION

The system includes following transactions:

- **Add records** would create patient's medical records in the DApp. It contains the fields of ID, name, co-morbid, blood group, and IPFS hash. The patient's basic medical records is stored along with the IPFS hash that contains the file uploaded containing the lab results or other medical records of patient.
- **Update records** would update the medical records of patient. This can only change the basic information of the patient not the IPFS hash. IPFS hash is non-updateable to ensure security of records.
- **View records** would let the user view the medical records of a patient stored in DApp. The view records function is used both by doctors and patients. The patient can view his records by the system authenticating that patient views only his own medical records. For this purpose system uses the public account address of the patient to ensure that only the relevant medical records is shown to the patient.
- **Delete records** would make the user be able to delete record of any patient. The user here would be the doctors they are given this right to delete any patient's record stored on the blockchain.
- **Grant access** for each of the above mentioned transactions, certain user would need to have access to them, i.e., only the doctor or nursing staff can make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities. Moreover, patient can view his medical records but won't be given the access to add or update them.

3) SYSTEM IMPLEMENTATION

As already explained in the previous sections, the system was implemented by using the Ethereum and its dependencies. This section explores system implementation in more detail to get an insight on the system various functions.

4) SMART CONTRACTS

As explained earlier, smart contracts are an important part of DApps as they are used for performing basic operations. Following contracts are included in this framework:

- Patient Records
- Roles

These contracts are used for giving access to the users on the DApp and performing CRUD operations on the records of patient. The *Patient Records* smart contract is made purely for implementing the functionality of the proposed framework.

It performs the CRUD operations along with the defining roles for access of these functions.

The second contract mentioned above, i.e., *Roles* is a predefined smart contract by the OpenZeppelin smart contract library. This library contains several smart contracts performing various functionalities that could be used for creating your own smart contracts. The reason behind using this library was to make use of the benefits it provides, i.e., tested and community reviewed code. The *Roles* smart contract belongs to the Asset library, which is a sub-library of the OpenZeppelin library. The asset library contains various other contracts for defining the access rules but roles library provide a granular role definition mechanism which was the main reason behind selection of this smart contract.

The algorithm for defining the *Patient Records* smart contract is given below. It defines all the operations that are being performed in it and various conditions that are associated with them. It also explains how the *roles* are being maintained for granting access to a particular functionality.

B. USAGE SCENARIO FOR ALGORITHM 1

The Algorithm 1 explains the functioning of the smart contract for patient records. This algorithm has five functions that are to define roles, add, view, update and delete records. These functions are used by the administrator and other users of the system. The first function of Algorithm 1 *define roles,* is to be performed by the administrator and it includes two variables new role and new account; these would be used for adding new role and account in role mapping list. This list would be used later on for accessing the roles of the users of the system. The second function is *add patient record* and it is performed by the doctor after they have been assigned this role by the administrator in the *define roles* function. This function also keeps a check that this task is being performed by the authenticated public address of the doctor's account and not by any other third party. For this they use 'msg.sender' term which in programming language, i.e., Solidity language used by Ethereum is used for identifying the address of the user. After this validity check is done the doctor can add the records of patient and after doing so would end the function by saving that record.

The third function is *view patient records* and it needs the patient id to be passed as the variable. This id would be used to by the system to look up the records of the patient and after doing so it would return those records to the account that requested to retrieve those records. This function also includes the validation for the assigned roles of patient or doctor. As only the patient and doctor would be allowed to view the records. The fourth function is *update patient records* and is used for making any changes in the saved records of the patient. The validation process is done once again to ensure that the authenticated users are accessing this function. The last function of Algorithm 1 is *delete patient records* which as evident from its name is used for deletion of the records of a specific patient. This function takes the unique id of

---

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:
function View 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

---

patient as input and after validating that the doctor is the one performing this function it would delete those records. This role based access would ensure that no third party is accessing these functions and only the authenticated users of the system would have access to these functions.

C. WORKING EXAMPLE FOR PROPOSED FRAMEWORK

As mentioned in previous section, we have used Ethereum for implementation purposes and the expected block time for it is between 10 to 19 seconds. Here by block time we are referring to the amount of time taken by a new block to be generated. For smart contracts the amount of time it takes for a transaction to be confirmed is 38 seconds and this depends upon the gas price specified for the transaction. Unlike Bitcoin, Ethereum has no block size limit but instead it has a gas limit, the terms gas price and gas limit are defined in the previous sections. The time taken for an append function of Algorithm 1, i.e.,*Add Patient Record*would be around 1-2 minutes depending upon the size of data. For the retrieval function such as Algorithm 1 function of *View Patient Record*would take 50 seconds.

In order to explain the functionality of Algorithm 1 in terms of transaction size let us consider the following example.

Let,

Number of transactions per hour (Avg) = 31474

Number of blocks per hour (Avg) = 269

Average transactions per block = Avg. number of transactions per hour / Avg. number of blocks per hour

= 31474/269 =117

Average transactions size = Block Size / Average transactions per block

= 21.7KB / 117 = 0.19 KB
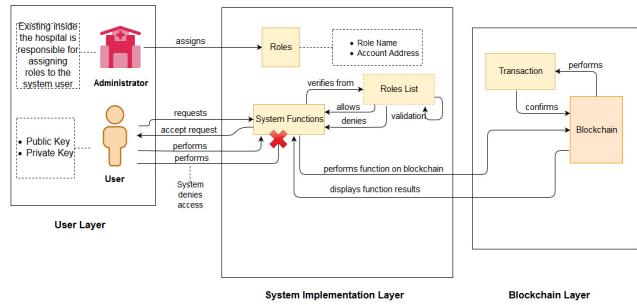
By the above calculations it is deduced that the average transaction size is 0.2 KB approximately. It should also be kept in mind here that these figures used above are real time values and are specifically for Ethereum blockchain network.

D. USAGE SCENARIO FOR PROPOSED FRAMEWORK

The figure 3 below depicts the basic usage scenario of the proposed framework. The system mainly has two entities, i.e., Administrator and User. Users are further divided into two categories for our proposed framework they are doctor and patient. These users are assigned roles by the administrator of the system who is someone belonging to the hospital's administrative staff. Here administrator is assigned the task of the defining the granular access to two main users of our system, i.e., doctor and patient.

So, the first activity would be that administrator assigns roles and this would include *Role Name* and *Account Address* of the user who is being assigned that role. Every user of this proposed system would have a role name and account address for using the system. So, after administrator assigns this user some role, that role name and account address is stored in a roles list for validation purpose required in later steps.

After roles are assigned, now when a *user* wants to perform some operations on the proposed system he would at first request to perform them. The system would verify the user role name and account address from the *Roles List* and allows them accordingly to perform those functions after validation returns success. After the functions are performed the system would store the information on the *Ethereum Blockchain* that

FIGURE 3. User interaction with DApp.

would perform transactions for that information. Once the transaction is confirmed the system receives the message of success from the blockchain layer that users can view on the DApp browser on which the whole proposed framework is being visible.

VI. PERFORMANCE

In this section we evaluate the performance of the proposed framework. By assessing the performance we can mitigate the risks associated with this novel technology that is understandable by very few individuals.

A. EXPERIMENTAL SETUP

For testing performance of the proposed framework we have conducted experiments by using the following configurations:

- Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHz processor
- And 8.00 GB of memory with Windows 64-bit OS (version 10)

We developed our proposed framework by using the Solidity which is programming language of Ethereum. JavaScript and Python are encapsulated in the Solidity language which is provided by the Ethereum to write code in smart contracts.

B. DATA COLLECTION FOR PERFORMANCE EVALUATION

This section explains what kind of data is used for evaluation of performance of the proposed framework. This section also discusses the metrics that are used to explain the results of this performance evaluation being conducted.

1) TRANSACTION DATA

To evaluate the performance of the proposed framework following transaction data with its details are used.

- **Transaction Deployment Time (t_{x1})**

It is defined as the time when transaction gets deployed. In Ethereum, a smart contract is deployed using the transaction so this deployment time refers to that time.

- **Transaction Completion Time (t_{x2})**

It is defined as the time when the transaction is completed and confirmed by the blockchain which in this case is Ethereum.

2) EVALUATION METRICS

The metrics used for evaluation include the execution time, latency and throughput of the proposed framework. These are explained briefly as follows:

- **Execution Time** is defined as time duration (in seconds) between the transaction confirmation and its execution in the blockchain network. Mathematically, it is (max (t_{x2}) - min (t_{x1})).
- **Throughput** refers to the amount of data that could be transferred from one location to another in a unit amount of time.
- **Latency** is known as the delay that occurs when a system component is waiting for another component of the system to respond to an action. In terms of time it could be referred as the difference of deployment and completion time of transaction.

C. RESULTS

1) PERFORMANCE ASSESMENT

In order to understand how our proposed framework would perform in real-case scenario of various users performing different functions on the framework we conducted performance evaluation using Apache JMeter version 5.1.1 and Apache Version 2.00. Apache JMeter is a desktop performance testing tool which is used for analysis and testing of applications [34].

a: AVERAGE EXECUTION TIME
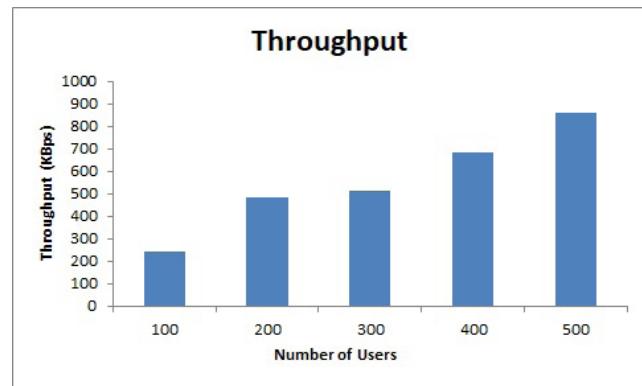
The execution time increases with the number of transactions being increased. These transactions are performed for the various functions that are included in the smart contract whose algorithm is defined in Section V. When there is only one user using the system the functions *Assign Roles, Add Patient Records* and *View Patient Records* would take 18.29 sec, 1 min 48 sec and 50 sec respectively for these functions to be executed. This time would increase when 100 users are using the system simultaneously.

b: THROUGHPUT

Algorithm 1 explains various functions that are included in the smart contract of the proposed framework. By using JMeter we simulated number of users from 100 users to 500 users (with period of 10 to 35), who are using the system and performing its various functions. In JMeter the throughput is represented in Data/time i.e. KB/sec units. While conducting the experiments we simulated the number of users as specified above and evaluated the performance of the system. These simulations are run on the proposed framework and at the end throughput is analyzed.

The following figure 4 shows the throughput of the proposed framework.

It is observed while conducting this experiment that as the number of users and requests increase the throughput of the system increased considerably in a linear manner. This
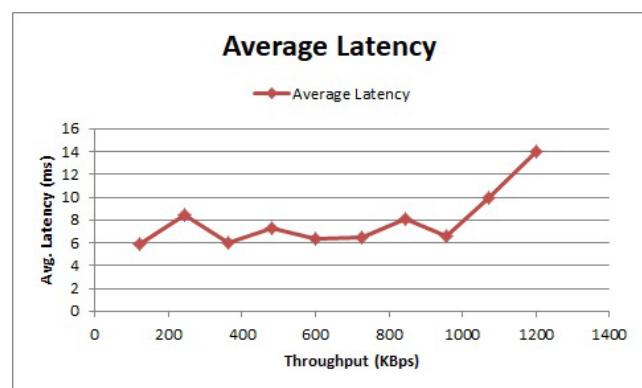
FIGURE 4. Throughput of the proposed framework.

linear increase in throughput indicates the efficiency of the proposed framework.

c: AVERAGE LATENCY

Latency as defined earlier is the delay or difference in time when one system component sends a request and a response is generated by any other system component. The difference between these two actions is defined as latency. Here we have evaluated the average latency of the proposed framework by using JMeter. While evaluating the latency of the proposed framework we simulated the number of users by JMeter. In JMeter latency is measured in terms of milliseconds.

The following graph Figure 5 gives an overview of average latency of the system along with the throughput of the proposed framework. The highest recorded latency in this experiment is 14ms.

FIGURE 5. Average Latency of the proposed framework.

We also evaluated the performance of the proposed framework by assessing the size and cost of the transaction. Before assessing the transaction size we also analyze the transaction payload. This assessment is discussed in detail in the following section.

2) PERFORMANCE EVALUATION (TRANSACTION)

Every transaction on Ethereum contains a data payload field. Data payload is included in that transaction which is meant

to invoke smart contract functions. This data payload is in the hex-serialized format and has bytes associated with it. Here we would discuss two functions from Algorithm 1 in order to understand the data payload included in the transactions being generated.

Data payload is the optional field of a transaction which is only used when there is some form of interaction with contract functions. It has two important parts,

- Function Selector
- Function Arguments

The *function selector* are first 4 bytes of Keccak-256 hash, it is used for identification of the smart contract function which is being invoked. The *function arguments* include various static and dynamic element types which have different rules for encoding them in payload.

Let us now understand the payload of *Define Roles* function from Algorithm 1 to get an understanding as to how the data payload is generated. Firstly we would separate the function selector and arguments. The function selector is actually the function signature which in this case is:

```
DefineRoles (string, address)
```

For the above function the Keccak-256 hash is as follows,

```
0x6c0abd24edce8ce20a2dfb1cd2026179214
468cde47681e871b6e14bf9d39efd
```

The first 4 bytes of the generated hash (*0x6c0abd24*) are of the function selector which points to the function being invoked from the contract. After function selector is calculated let us now understand how the function arguments are encoded.

For this we encode the head part of two arguments, the *address* is the static type and *string* is the dynamic type. The static type is passed directly while for dynamic type the offset in bytes are used, it is also measured from the start of the value encoding. The first four bytes containing the hash of function signature is not counted in it.

The encoding for dynamic type *string* with value "Doctor" would be as follows,

```
0x000000000000000000000000000000000000
000000000000000000000000006
```

The number of elements or bytes is 6 and they are represented as seen above. Following is the string value "Doctor" padded to 32 bytes on the right.

```
0x48976c7c7f2c20667f626c6421000000000
0000000000000000000000000000
```

TABLE 2. Data payload of transactions used in proposed framework.

Data Payload	Contents Types	Size
Payload of F_{assign}	string, address	64 bytes
Payload of F_{add}	string, string, string, string, string, address	192 bytes
Payload of F_{view}	string, uint	64 bytes
Payload of F_{update}	string, uint, string, string, string	160 bytes
Payload of F_{delete}	string, uint	64 bytes

TABLE 3. Transactions size and fee for proposed framework.

Transaction	Size	Fee
TxF_{assign}	132 bytes	0.00006 ETH
TxF_{add}	548 bytes	0.0003 ETH
TxF_{view}	122 bytes	0.0004 ETH
TxF_{update}	420 bytes	0.00001 ETH
TxF_{delete}	132 bytes	0.0003 ETH

The encoding of this function with only its dynamic types is as follows,

```
0x6c0abd24
  0x000000000000000000000000000000000
  00000000000000000000000000000006
  0x48976c7c7f2c20667f626c64210000000
  000000000000000000000000000000
```

The static and dynamic type in this function would have size of 32 bytes. The total byte size of this function is 64 bytes. In the same way we can calculate the data payload of other functions of the Algorithm 1. The following table 2 represents the data payload size of various functions.

By using the data payload we can calculate the transaction sizes of various functions of our proposed framework. Table 3 represents the transaction sizes in bytes for these functions. Here it must also be kept in mind that the transaction size calculated in this section is from data payload perspective and is specifically calculated for various functions of Algorithm 1, where as in Section V the transaction size was calculated from block size perspective and was calculated in a generalized manner.

We can also calculate the fee or cost associated with various transactions of the proposed framework. In Ethereum the transaction fees is calculated in 'ETH' [29] which is Ethereum coin and it has certain units such as wei, gwei associated with it. The formula to calculate Ethereum transactions fee is also discussed here. The transaction fee for a transaction is the product of gas consumed and gas price. It could be represented as follows,

$$Transaction\ Fee = gasConsumed \times gasPrice$$

We can calculate the transaction fee by using the recommended figure for gas consumed which is 21000 and is 21 Gwei for gas price. So,

$$Transaction\ Fee = 21000 \times 21 = 441000\ Gwei$$

And to calculate the transaction fee of 1ether we would use the following method,

$$1\ Ether = 1000,000,000\ Gwei$$
$$Transaction\ Fee\ for\ 1\ Ether = 441000/1000,000,000\ Gwei$$
$$= 0.00041\ Gwei$$

The transaction fees for various functions of Algorithm 1 are presented in table 3.

3) COMPARISON OF PROPOSED FRAMEWORK WITH RELATED WORK

We also discuss some parameters that are present in our framework and are used for comparison with the related work in this domain. While ensuring the presence of these parameters in the framework it is also considered that it would not compromise the security and privacy of the system. For this both security and privacy are discussed in each of the parameters discusses below.

A. SCALABILITY

Scalability in simpler terms refers to the ability of an information system to perform it functions well in such situations when the storage volume of the system increases or decreases. In case of blockchain technology scalability is an issue that needs some permanent solution. As data size or volume is increasing on the blockchain. Our proposed system used the off-chain storage mechanism as the patient's data stored on the blockchain contains the basic information of patient along with the IPFS hash, i.e., the off-chain scaling solution used in our proposed system framework. This solves the scalability issue mentioned as now huge volume of patient medical record is not stored on the blockchain. As, the data size being stored on the blockchain has now decreased the transactions could also be performed faster. As mentioned earlier, IPFS uses cryptographic hash which is stored in the decentralized manner using peer-to-peer network. This also ensures that while solving the scalability problem the security of the framework is not compromised.

B. CONTENT-ADDRESSABLE STORAGE

Content-addressable storage refers to the off-chain storage mechanism of IPFS used in the proposed framework [20]. The sensitive record of patient is stored on the IPFS, which ensures that a hash of the stored record is generated. That hash is now stored in the blockchain and is accessed when needed by the doctors and patients. The IPFS generates the cryptographically secure hash which ensures the security of the data being stored on it. And this also ensures security in our proposed framework.

TABLE 4. Comparison of proposed framework with related work.

	[24]	[25]	[26]	**Our Proposed system**
Blockchain-based	Y	Y	Y	Y
Scalability	Y	Y	N	Y
Content-Addressable Storage	N	N	N	Y
Integrity	Y	Y	Y	Y
Access Control	N	Y	Y	Y

C. INTEGRITY

Integrity of a system is measured by the trustfulness of that system and also that system storing that information is temper-proof and reliable. This blockchain-based system ensures that it does not compromise this feature. The information stored in this system is intact and is not changed by any unauthorized channel. Moreover, information is available to only the associated parties that are doctors and patients. The users of the system and any third party do not have the right to make any changes in the smart contract as they are not having any access to it. This is done by using the access rules which ensure that the private data or medical records of patients are not accessible and remain temper-proof. Moreover, using IPFS for storage of records also ensures the security of the medical records of the patients.

D. ACCESS CONTROL

Using the Role-based access mechanism, this framework makes sure that every entity of the system is assigned a role. Any third party who is not authorized to have access to the system would not be able to access the system. This system provides a two core security as firstly blockchain technology in itself is secure and uses certain protocols and mechanism to keep itself secure from third-part intrusions. And secondly our system uses the Role-based access that also only allows the users having defined roles to have access to the system and its functions. So, our system would not only ensure security of patient records but would also make sure the access control of entities associated with it. This parameter also ensures that the security of the patient's personal medical data is not compromised and the access is provided to only the authorized users of the system.

E. INFORMATION CONFIDENTIALITY

The patient medical records stored on the blockchain should be secured from any third party access to ensure the confidentiality of the patients' record. The patient's data include the important information of patient such as the patient medical history, blood group, records, lab results, X-rays reports, MRI results and many other related results and reports. All of this information is critical not only to patients but also to the hospital. Smart contracts are a really helpful element in this system as they ensure transparency, precision and trust on

the transactions being performed. The record being stored and accessed in the system are only accessible by the trusted parties. Any untrusted third party trying to access the system is denied access by the system. With the information being kept as confidential from third party access the framework would ensure that it would the aspect of privacy as well.

VII. CONCLUSION AND FUTURE WORK

In this paper we discussed how blockchain technology can be useful for healthcare sector and how can it be used for electronic health records. Despite the advancement in healthcare sector and technological innovation in EHR systems they still faced some issues that were addressed by this novel technology, i.e., blockchain. Our proposed framework is a combination of secure record storage along with the granular access rules for those records. It creates such a system that is easier for the users to use and understand. Also, the framework proposes measures to ensure the system tackles the problem of data storage as it utilizes the off-chain storage mechanism of IPFS. And the role-based access also benefits the system as the medical records are only available to the trusted and related individuals. This also solves the problem of information asymmetry of EHR system.

For the future, we plan to implement the payment module in the existing framework. For this we need to have certain considerations as we need to decide how much a patient would pay for consultation by the doctor on this decentralized system functioning on the blockchain. We would also need to define certain policies and rules that comply with the principles of the healthcare sector.

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.

[2] K. Wisner, A. Lyndon, and C. A. Chesla, "The electronic health record's impact on nurses' cognitive work: An integrative review," *Int. J. Nursing Stud.*, vol. 94, pp. 74–84, Jun. 2019.

[3] M. Hochman, "Electronic health records: A "Quadruple win," a "quadruple failure," or simply time for a reboot?" *J. Gen. Int. Med.*, vol. 33, no. 4, pp. 397–399, Apr. 2018.

[4] Q. Gan and Q. Cao, "Adoption of electronic health record system: Multiple theoretical perspectives," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 2716–2724.

[5] T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen, A. M. Aalto, and T. Heponiemi, "Experienced time pressure and stress: Electronic health records usability and information technology competence play a role," *BMC Med. Inform. Decis. Making*, vol. 19, no. 1, p. 160, Aug. 2019.

[6] M. Reisman, "EHRs: The challenge of making electronic data usable and interoperable.," *PT*, vol. 42, no. 9, pp. 572–575, Sep. 2017.

[7] W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, "Electronic health record breaches as social indicators," *Social Indicators Res.*, vol. 141, no. 2, pp. 861–871, Jan. 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. Making*, vol. 19, no. 1, p. 10, Dec. 2019.

[9] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decis. Support Syst.*, vol. 108, pp. 57–68, Apr. 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, Jul. 2018.

[11] "The future of health care cybersecurity," *J. Nursing Regulation*, vol. 8, no. 4, 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, Aug. 2019, Art. no. 101144.

[13] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electrnic Cash System*. 2008, pp. 1–9.

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

[15] A. Boonstra, A. Versluis, and J. F. J. Vos, "Implementing electronic health records in hospitals: A systematic literature review," *BMC Health Services Res.*, vol. 14, no. 1, Sep. 2014, Art. no. 370.

[16] 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, p. e3, Jan./Mar. 2005.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[18] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: The next generation of medical records?" *J. Med. Syst.*, vol. 42, no. 9, p. 172, Sep. 2018.

[19] 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, Jan. 2019.

[20] J. Eberhardt and S. Tai, "On or off the blockchain? Insights on offchaining computation and data," in *Proc. Eur. Conf. Service-Oriented Cloud Comput.*, Oct. 2014, pp. 11–45.

[21] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2018, pp. 1–6.

[22] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 108–113.

[23] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[24] M. S. Sahoo and P. K. Baruah, "HBasechainDB—A scalable blockchain framework on Hadoop ecosystem," in *Supercomputing Frontiers*. 2018, pp. 18–29.

[25] 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, Jul. 2018.

[26] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, "Sharing medical questionnaires based on blockchain," *Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM)*, Dec. 2018, pp. 2767–2769.

[27] S. Gupta and M. Sadoghi, "Blockchain transaction processing," in *Encyclopedia of Big Data Technologies*. 2019, pp. 366–376.

[28] U. W. Chohan, "Cryptocurrencies: A brief thematic review," *SSRN Electron. J.*, 2017.

[29] G. Wood, "Ethereum: A Secure Decentralised generalised transaction ledger. EIP-150 revision," Tech. Rep., Aug. 2017, p. 33.

[30] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, "SoK: Unraveling bitcoin smart contracts," in *Proc. Int. Conf. Princ. Secur. Trust*, Thessaloniki, Greece, 2018, pp. 217–242.

[31] I. Grishchenko, M. Maffei, and C. Schneidewind, "A semantic framework for the security analysis of ethereum smart contracts," in *Principles of Security and Trust*. 2018, pp. 243–269.

[32] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "HealthSense: A medical use case of Internet of Things and blockchain," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2017, pp. 486–491.

[33] *InterPlanetary File System (IPFS)*. Accessed: Feb. 4, 2019. [Online]. Available: https://ipfs.io/.

[34] M. Niranjanamurthy, K. Kumar S, A. Saha, and D. D. Chahar, "Comparative study on performance testing with jmeter," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 2, pp. 70–76, 2016.

AYESHA SHAHNAZ received the B.S. degree in computer science from the Capital University of Science and Technology (CUST), Islamabad. She is currently pursuing the M.S. degree in software engineering from the College of Electrical and Mechanical Engineering, National University of Science and Technology (NUST), Islamabad. She was a Lab Instructor with the Department of Computing, CUST. Her current research interests mainly include the blockchain development, data, and text mining.

USMAN QAMAR received the master's degree in computer systems design from the University of Manchester Institute of Science and Technology (UMIST), U.K., the joint M.Phil. degree in computer systems from UMIST and the University of Manchester, which focused on feature selection in big data, and the Ph.D. degree from the University of Manchester, U.K., in 2009. His Ph.D. specialization is in data engineering, knowledge discovery, and decision science. His Post-Ph.D. work with the University of Manchester, where he involved in various research projects, including hybrid mechanisms for statistical disclosure (feature selection merged with outlier analysis) for Office of National Statistics (ONS), London, U.K., Churn Prediction for Vodafone U.K., and customer profile analysis for shopping with the University of Ghent, Belgium. He has done a Postgraduation in medical and health research from the University of Oxford, U.K., where he worked on evidence-based health care, thematic qualitative data analysis, and healthcare innovation and technology. He has also successfully supervised four Ph.D. degree students and more than 70 master's degree students. He has been able to acquire nearly PKR 100 million in research grants. He is currently the Director of the Knowledge and Data Science Research Centre, the Centre of Excellence with NUST, Pakistan, and the Principal Investigator of the Digital Pakistan Lab, which is part of the National Centre for Big Data and Cloud Computing. He has more than 15 years of experience in data engineering and decision sciences both in academia and industry having spent nearly ten years, U.K. He has also authored more than 150 peer-reviewed publications which includes two books published by Springer & Co, five book chapters, 36 impact factor journal publications with a combined impact factor of 91.98 (Clarivate Analytics Impact Factor), and more than 100 Conference Publications. He was also a recipient of the prestigious Charles Wallace Fellowship, in 2016 and 2017, as well as a British Council Fellowship 2018, a Visiting Research Fellow with the Centre of Decision Research, University of Leeds, U.K., and the Scientific Director of the Data and Text Mining Lab, Manchester Metropolitan. He is an Expert Committee Member of engineering and technology for the evaluation/recognition of national research journals for Higher Education Commission (HEC), Pakistan. Because of his extensive publications, he is a member of Elsevier Advisory Panel. Many of his articles have been awarded best research article awards by Higher Education Commission, Pakistan. He was a recipient of multiple research awards, including the Best Researcher of Pakistan, in 2015 and 2016, by Higher Education Commission (HEC), Pakistan, the Best Overall NUST University Researcher Award, in 2016, and the Best College of E&ME Researcher Award, in 2016, as well as the Gold in Research and Development category by Pakistan Software Houses Association (P@SHA) ICT awards, in 2013 and 2017, and the Silver Award in APICTA (Asia Pacific ICT Alliance awards), in 2013, in category of Research and Development hosted by Hong Kong. He has the honor of being the finalist of the British Council's Professional Achievement Award, in 2016 and 2017.

AYESHA KHALID received the B.E. degree in computer systems engineering from the National University of Sciences and Technology (NUST), Pakistan, and the M.S. degree in electrical engineering from the Center for Advanced Studies in Engineering (CASE), University of Engineering and Technology, UET-Taxila. She is currently a Lecturer with Queen's University of Belfast, Belfast, U.K. Her research interests include lattice-based cryptography, embedded systems security, side channel attacks, and cryptographic hardware. She was a recipient of the DAAD Scholarship Award for her Ph.D. studies at RWTH Aachen, Germany.

● ● ●