A Framework for Secure Healthcare Data Management using Blockchain Technology

Ahmed I. Taloba, Alanazi Rayan, Ahmed Elhadad, Amr Abozeid, Osama R. Shahin, Rasha M. Abd El-Aziz
Department of Computer Science, College of Science and Arts in Qurayyat, Jouf University, Saudi Arabia

***Abstract*—In the current era of smart cities and smart homes, the patient's data like name, personal details and disease description are highly insecure and violated most often. These details are stored digitally in a network called Electronic Health Record (EHR). The EHR can be useful for future medical researches to enhance patients' healthcare and the performance of clinical practices. These data cannot be accessible for the patients and their caretakers, but they are readily available for unauthorized external agencies and are easily breached by hackers. This creates an imbalance in data accessibility and security. This can be resolved by using blockchain technology. The blockchain creates an immutable ledger and makes the transaction to be decentralized. The blockchain has three key features namely Security, Transparency, and Decentralization. These key features make the system to be highly secured, prevent data manipulation, and can only be accessible by authorized persons. In this paper, a blockchain-based security framework has been proposed to secure the EHR and provide a safe way of accessing the clinical data of the patients for the patients and their caretakers, doctors, and insurance agents using cryptography and decentralization. The proposed system also maintains the balance between data accessibility and security. This paper also establishes how the proposed framework helps doctors, patients, caretakers, and external authorities to securely store and access patients' medical data in EHR.**

Keywords*—Blockchain; electronic health record (EHR); storage; security; accessibility; cryptography; decentralization*

I. Introduction

In the modern world, medical data sharing leads to the discovery of new techniques and treatments for curing several diseases. This can be done by storing the medical data digitally and by facilitating remote accessibility. The data stored in the electronic record is from the patients after visiting the hospital and making them the only owner of such records. The number of data stored in the electronic records is going on the increase and forms big data which can be used for several purposes in the healthcare domain. The vitality of data storage and sharing gives rise to several business entities for collecting, processing, analyzing, and storing the data to share them with other authorized sectors. This process increases several business organizations to focus on cloud storage and processing, data analytics, and provenance that renders existing organizations depending on the availability of data to operate and for their existence. To achieve the high demand in big data storage, several stakeholders invested in cloud computing and storage. This storage attracted the interests of several users including the patients, healthcare sectors, and research sectors for data storage in cloud repositories and provides controlled, cross-domain and flexible sharing of data to the beneficiaries. The major challenge in cloud data storage and sharing is the risk of the data being exposed to unauthorized third parties [1].

With the fundamental development of information and telecommunication technology, health-related services have been brought to the patient's doorstep with the help of the Telecare Medicine Information System (TMIS). The TMIS can help doctors to provide medical support from any remote location by discussing with patients about their illness and also by sharing critical information with other medical experts. In this way, the TMIS can reduce the treatment cost drastically. This system facilitates accurate decision-making in disease diagnosis by accessing up-to-date medical history. But the limitation here is the decision-making for new patients whose medical history and other related data are not available in health records. This can be overcome by using the EHR which holds all the data such as patient's details, scan reports, clinical notes, sensor data, billing details, medications, medical history, insurance details, and other related information. This type of record would suffer privacy and security issues in data-sharing [2]. Recently, wearable device technologies and the Internet of Things (IoT) have been evolving in the healthcare sector. Data from each wearable device were stored in the cloud which can provide big health data and valuable visions. This data is linked with the EHR to improve monitoring the heath, diagnosing the disease, and in the treatment of diseases [3].

The Electronic Medical Record (EMR) is a systematized digital record that holds the healthcare details of patients and populations. The initial perspective of EMR is to replace the traditional paper-based medical records and to enhance hospital data management in healthcare sectors. After that, the increase in the self-health concern, the general population also needed to access health records of their own. Hence, a novel personalized data management of healthcare information has been introduced, which is named Electronic Health Record (EHR) [4].

The EHR and EMR are offering improved security and user experience along with other healthcare-related aspects. Still, some security concerns have been believed to be resolved using Blockchain technology. The blockchain in the healthcare sector provides a secure and temper-proof system for recording medical data. This technology can also prevent inefficiency, insecurity, non-temper-proof, unorganized nature, duplication, and redundancy of data that occurs from the paper-based medical record [5]. State of transactions must not be easily detectable back to the relevant patient populations, according to advocates for transaction privacy on the

blockchain. To do so suggests using tokenization, which is a method of making only a representation to the sensitive material public while keeping the raw, confidential data private. Furthermore, it designates the need for health records to be securely stored off the blockchain. Since this blockchain is frequently used to store references to records stored in an access database, the database should be protected in and of itself. Our architecture protects the information both on blockchain as well as in the database by encoding information in the database.

An EHR is an electronic version of the patient's medical history which includes the patient's clinical data obtained from demographics, progress reports, problems, symptoms, immunization reports, medications, radiology reports, laboratory reports, and immunization reports. Recording the patient details in a paper-based report leads to an extensive paper trail in many healthcare organizations and hence, they are moved to EHR. The EHR should satisfy the requirements like accomplishing whole data, flexibility to failure, being available at any time, and beinging reliable to security guidelines [6]. In the current decade, various technologies have been used to secure patients' private data from healthcare sectors. The healthcare data of a patient includes the patient's details, their height, weight, symptoms of disease-affected, and previous medical history. This medical data grows with time. The data recorded in electronic health records are simple data points but difficult to manage. This record has been generated, stored, and manipulated by several stakeholders for proper patient care and the effective use of such medical records. These stakeholders get authorization whenever they need the data. The EHR is made of the parameters as shown in Fig. 1 [7].

Blockchain consists of a continuous sequence of blocks that stores all the records like a conventional public ledger. A block consists of only one parent block with a block header that holds the previous block hash value. The Ethereum blockchain also stores the uncle block hash values. The first block is called the genesis block. The genesis block has no parent blocks. The block header is given in Fig. 2.

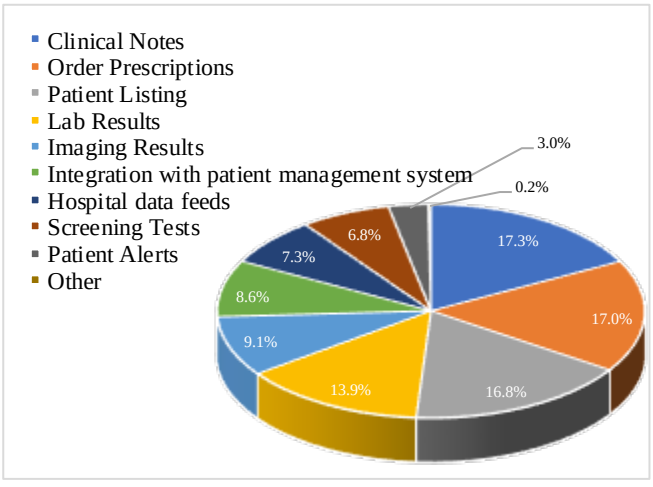

Fig. 1. Parameters of HER.

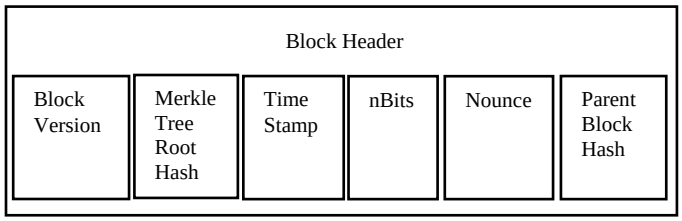

Fig. 2. Structure of Block Header.

Block version - Set of rules for block validation.

Merkle tree root hash - hash value of all records in a block.

Timestamp - Current time in seconds. Universal time since 1-Jan. 1970.

nBits - Target threshold value.

Nonce - 4-byte field starting from 0 and incremented while calculating each hash.

Parent block hash - Hash value with 256-bit pointing to the previous block.

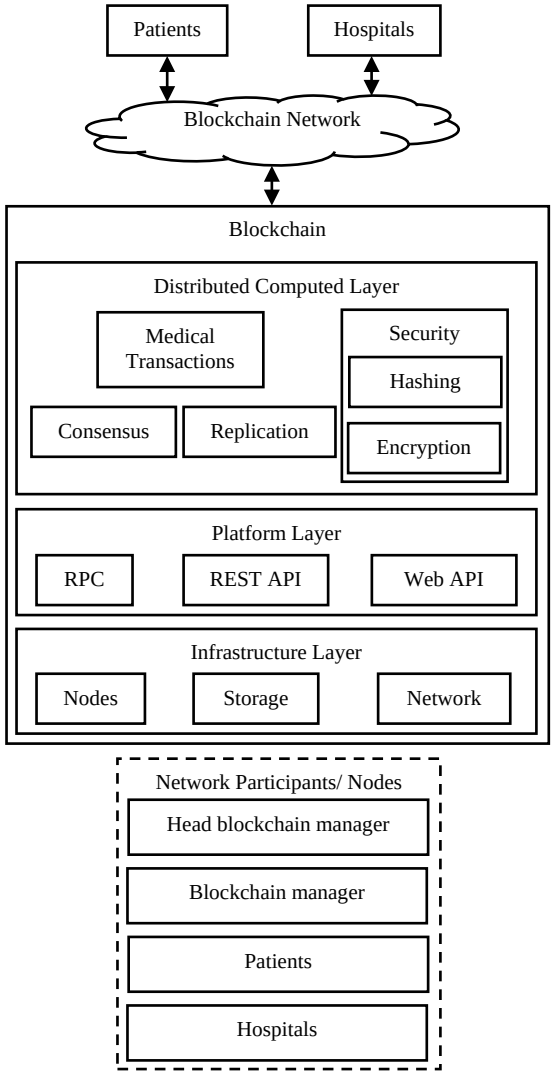

Fig. 3. Architecture of Blockchain Network in Healthcare Data Management.

While blockchain technology has many benefits for an EHR management system, it also has some drawbacks. The primary limitation of blockchain technology is that if % of the system's processing elements collide, the chain structure could be rewritten. To realize the benefits of a decentralized system, group members would have some confidence that at least mining nodes would not like to compromise the blockchain's immutability. Second, while using a permissioned blockchain undermines the incentive of external forces to connect PHI, it cannot hide transaction records. This gives nodes the ability to perform unfavorable network analysis. An adversary may indeed be able to identify the frequency through which a particular node attends a physician or the providers or third parties with whom a focus of previous associates by analyzing blocks of transactions. Finally, because cryptographic algorithms are distributed systems, their operation has a high memory usage. As a result, large amounts of data cannot be retained efficiently on the blockchain. As a result, while blockchains could be used for access management and data integrity, the information itself will be stored somewhere else and may be open to attack unrelated to the blockchain.

In a trustless environment, an asymmetric cryptography-based digital signature has been used throughout the network. Each user has a pair of private and public keys. The digital signature includes the signing and verification phase. The signing phase involves sharing the encrypted data with the private key and the original data. The verification phase involves validation of the data with a public key, whether it has been tampered with or not. The key characteristics of the blockchain are decentralization, persistency, anonymity, and suitability [8]. Fig. 3 shows the architecture of a blockchain network in healthcare data management.

Here, API – Application Programming Interface

RPC – Remote Procedure Calls

REST – REpresentational State Transfer

The traditional method is a Client-Server architecture or Singleton approach. The client is the end-user. The server gets the requests from the client which are then processed and the result will be forwarded to the client. A single authority (Server) will control the whole process. Whenever there is an attack on the server, the whole system will be collapsed. The modern Blockchain technology consists of data split over several systems. Each system is called a node. All the data are stored in a block that is connected via links formed by hash values. To calculate the hash value, the transaction in a block and the hash value of the previous block have been used [9].

The currently using healthcare data management involves centralized servers which seek permission to access multiple entities of medical data in a network which leads to delayed services and can be suspected to leakage of such information. Most of the patients are unaware of which entity stores and uses their medical data in such healthcare systems. The major challenge in this system is the security while accessing the data with various entities within the network. In such cases, Blockchain technology can be used to secure the accessibility and integrity of healthcare-related information [10].

The remaining sections in this paper cover the Related Works which describes the existing approaches that use blockchain in the management of healthcare data in Section 2, followed by the Proposed Methodology in Section 3, then Result and Discussion part in Section 4, and finally, the paper concludes in Section 5.

II. Related Work

A secure cloud-based EHR system has been implemented to accomplish confidentiality, authenticity, and integrity of healthcare data and to facilitate data sharing with the help of the C-AB/IB-ES scheme and blockchain. This system uses 5 entities namely key generation center, hospital, patient, cloud, and users who access the data. At first, the patients sign the health-related data and authorize the hospitals to access their data. This authorization letter will be submitted to the blockchain data pool and wait for consensus node processing. The hospital then encrypts the data and submits it to the data pool with the hospital's signature. The consensus node monitors the data pool and captures the matched authorization letter and the encrypted data. The signature is verified to make sure that the data is completed and with the patient's authorization. Then a consensus protocol would be performed to select a bookkeeping node that submits the encrypted data to the cloud along and the data description and its address were also written to the blockchain [11]. A prototype has been developed and implemented in a mobile platform for data sharing using Amazon cloud computing. This application uses the combination of blockchain and the decentralized Interplanetary File System (IPFS). The Ethereum blockchain has been used to demonstrate the performance of the developed Android mobile application. An Ethereum blockchain has been employed to build the e-healthcare system. Ethereum is a new distributed blockchain network like Bitcoin. The most significant merit of Ethereum is its adaptability and flexible nature which can be used to build an application using blockchain [12].

A permission blockchain network has been implemented for healthcare data management to overcome the issues associated with the permission-less blockchain network. This is because the permissioned blockchain network can overcome the problems like unauthorized network participation which causes impersonation of members, clear transaction data which includes the sensitive and confidential data of the patients that can be accessed by all the members in that network, network throughput is slow which hinders the treatment for patients, limited usability due to the payment for transaction and mining rewards. Also, the permissioned network prevents the demerits of permission-less networks such as high energy consumption, limited scalability, and low transaction throughput [13]. A survey on the investigation of the privacy and security issues while using wearable devices in the healthcare domain is given in [14]. For this survey, wearable healthcare devices have been designed and developed to collect the health-related data of the patients. By analyzing this data, the health status of a patient can be retrieved. The approach followed in this survey is the cross-sectional approach. This survey collected data from 106 respondents. Among them, 50% of respondents don't know the privacy concern in the healthcare data. The respondents

are also unaware of the security issues in the data collected using wearable devices. This survey finally suggests that the patients who are using the wearable devices should be educated about the privacy and security concerns in using them.

A new personal healthcare record sharing system with blockchain-based data integrity verifiable has been implemented in [15]. This scheme aims in resolving the issues that persisted in sharing the healthcare records like privacy disclosure, ability to search using limited keywords, loss in access control rights to share the personal health record. These issues have been overcome by using the techniques like searchable symmetric encryption and encryption based on attributes. This scheme varies from the existing methods in the way, that it uses an attribute private key to be distributed by the patients which avoids several problems that cause security issues in the existing systems. Also, this scheme uses blockchain to manage the keys which prevent the single-point failure issue in the management of centralized key. The efficiency of the data integrity verification has been improved by storing the hash value of the encrypted health data in the blockchain and storing the index set in the smart contract.

A blockchain-based access control manager for managing healthcare-related data has been described in [16]. This system is believed to overcome the challenges faced in interoperability by the industries stated by National Coordinator for Health Information Technology's (ONC) Shared Nationwide Interoperability Roadmap. Interoperability is one of the vital constituents for any structures that support Precision Medicine Initiative (PMI) and Patient-Centered Outcomes Research (PCOR). For access control management, this system uses a public blockchain for the data stored off-blockchain. Published research from the Massachusetts Institute of Technology has been borrowed to analyze the management and access control of personal data in a public blockchain. An implementation of a framework called Decentralized Application (DApp) in a private blockchain network platform using backend Distributed File System (DFS) has been given in [17]. The DApp is now using Proof-of-Work (PoW) consensus algorithm and is later suggested to use Delegated Proof-of-Stack (DPoS) consensus algorithm or Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. This system uses Ethereum for implementing the smart contract-based healthcare blockchain. This application can easily detect anomalies, missing data, and the insertion of unauthorized data. The major elements used in the smart contracts are the events, functions, modifiers, and state variables which were inscribed via a high-level programming language called Solidity. To deploy the smart contract in test-net and test-net ethers, Remix and Kovan test network was applied to pay the fee for the transaction. There are three stages in creating a smart contract using Solidity, namely the writing, compiling, and then announcing. The real-time solidity compiler generates the bytecode and Ethereum Wallet is used in announcing the smart contracts to the blockchain.

The framework proposes prioritizes secure communication and contains several contributions aimed at improving privacy and interoperability. To begin, unlike other blockchain EHR systems that have been proposed, the blockchain stores hashing algorithms of data references while sending the real request network information in a private exchange over the framework. Our framework uses proxy re-encryption to simplify the secure transmission of EHRs, but it lacks techniques like private transactions for privacy. Furthermore, we can store keys and small encoded records straight on the blockchain using proxy re-encryption, making it easier to transfer records like prescribing to dispensaries or even other third parties. This eliminates the need for users to store keys locally, allowing patients to eliminate access permissions if preferred.

A review of Healthcare Information Management Systems (HIMS) based socio-technical issues has been performed and found the problems such as low privacy and security, lack of data transparency, data integrity and accessibility, errors in the prescription of medication and supply chain, and lack of knowledge interpretation. This review also provides the possible solutions in identity and risk management, auditing functions, and solutions for privacy and security issues using blockchain technology. Also, it provides some recommendations for future research and development of HIMS [18]. Model Chain, a healthcare predictive modeling framework for decentralized privacy-preserving in private blockchain network has been demonstrated which uses privacy-preserving online machine learning algorithm adopting blockchain technology, in which the transaction metadata has been applied for distributing the partial model and also designed a proof-of-information system for finding the order of online learning process. This approach aims to improve the interoperability among the organizations to support Nationwide Interoperability Roadmap and national healthcare delivery priorities such as Patient-Centered Outcomes Research (PCOR) and to find the solution for privacy-preserving healthcare predictive modeling by using a peer-to-peer network like blockchain [19].

The health information that is monitored and transmitted by the remote health monitoring devices through IoT has been protected by applying the smart contract mechanism based on blockchain technology to enable secure managing and analyzing the data obtained from medical sensors. Ethereum protocol is applied to a private blockchain network to make the medical sensors communicate with smart devices which call the smart contract and record the events completely into the blockchain network. The use of such a smart contract system facilitates real-time monitoring of patients and their medical data by transmitting them as notifications to the hospitals and patients in a highly secured platform. This approach can solve several security issues occurring in remote health monitoring of patients and automatically notifies the parties involved in the process in a HIPAA-compliant manner [20].

III. Proposed Methodology

The EHR has been managed by the healthcare institutions instead of the respective patients. This leads to difficulty for other health centers to access the patient details to provide perfect medical advice to the patients. Hence, the patients need to retain their health information for future access. The blockchain allows to store the healthcare data and provides

free access to the EHR via corresponding data providers and websites [21]. The proposed system develops a security framework for EHR which provides access to multiple authorities in a shared system using blockchain. Fig. 4 demonstrates the process flow of the proposed framework for healthcare data storage and access.

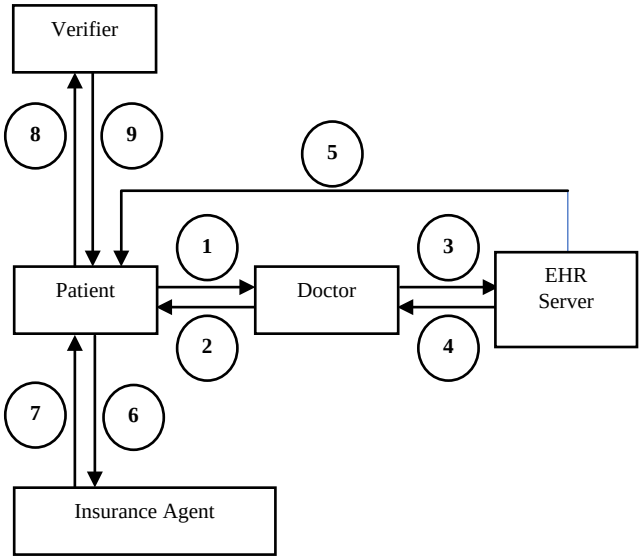

Fig. 4. Proposed Blockchain Framework for Healthcare Data Storage and Access.

The proposed blockchain framework enables the patients to directly access their data from EHR and can able to download and share them. There are 5 parties involved in the multi-user system. They are the Patient, Doctor, EHR Server, Insurance Agent, and the Verifier. The steps involved in the storage and sharing of patient's medical and personal data are given as follows:

1) The patient consults the doctor.

2) Treatment has been given to the patient by the doctor.

3) The EHR Server is a node present in the blockchain network which serves as a miner who collect the transaction data and store them as blocks. After creating the EHR, they are verified by all the nodes in the blockchain network whether it is a valid one or not. These transactions are stored in a memory pool which acts as a waiting area for all the transactions performed on each node and maintains those details within their node. The miner node collects this transaction information and forms it into blocks. The verification of such data can be done by using the hash, which is a 256-bit number that represents unique data. Once the verification got completed, the miner picks it from the memory pool and inserts them into a new block which will then be submitted to the blockchain.

4) Once the block is created, it will be distributed by the miner to all the nodes available in that blockchain network.

5) Access control has been provided to each of the nodes within the network. The proposed framework works in a way that the information of each patient will be secured by them. It means, the patient's details can be accessed by patients and also the doctor who gives treatment to them. This can be done only with the permission of that patient.

6) This data when claimed for insurance purposes, then it will be shared by the doctor who treated that patient to the insurance agent.

7) The insurance agent can refer the EHR of the patients, only who claimed from them and can approve the insurance payment to the patient.

8) The patient then sends the request for the verification of their data to the data verifier.

9) The verifier finally verifies and approves whether the data provided are safe and secured or not and delivers a verification result to the patients.

This framework allows only the patients to view their data in EHR. When a patient permits the doctor who treats them, then that doctor can also view the data. Likewise, the insurance agent can view only the data of the patient who claims insurance amount from them.

Algorithm-1: Formation and addition of Patient Blockchain

Input: Details of Patient for EHR

Output: Forming Patient blockchain and adding blocks to it

- Provide the medical data of the patient to the EHR
- Generate private and public keys using RSA cryptography technique
- The public key is used by the patients for encryption and the private key is for decrypting the encrypted data, by the doctor and insurance agent
- Generate the Hash for Encrypted EHR based on HMAC-SHA1 Algorithm
- With the help of the patient's ID, generate a Bilinear Map for the Encrypted EHR
- With the help of the Patient's name, ID and password, create a genesis block for the Patient
- Add the Encrypted EHR and Hash with Bilinear Map to the Block
- Add this block to the patient blockchain.

Algorithm-1 gives the formation and addition of Patient Blockchain. A Bilinear Map is used to enhance the security of the proposed framework. A function that combines 2 vectors to get a new vector is called the bilinear map which can be mathematically represented as:

$\overrightarrow{v_1} \times \overrightarrow{v_2} \rightarrow y$

Here, $\overrightarrow{v_1}$ = Encrypted EHR

$\overrightarrow{v_2}$ = Patient ID

y = Bilinear Map

This bilinear map is generated using the concept of identity-based encryption. Fig. 5 shows the Patient blockchain which consists of a genesis block with the patient's name, ID, and Password. The treatment taken by the patients has been added as a new block one by one. Only the patient can view the data stored in the patient blockchain, other than that no one can view it.

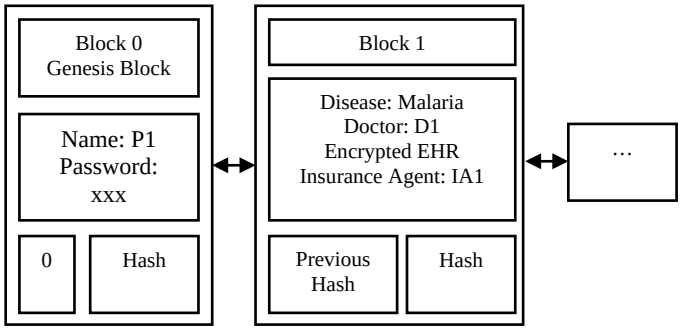

Fig. 5. Patient Blockchain.

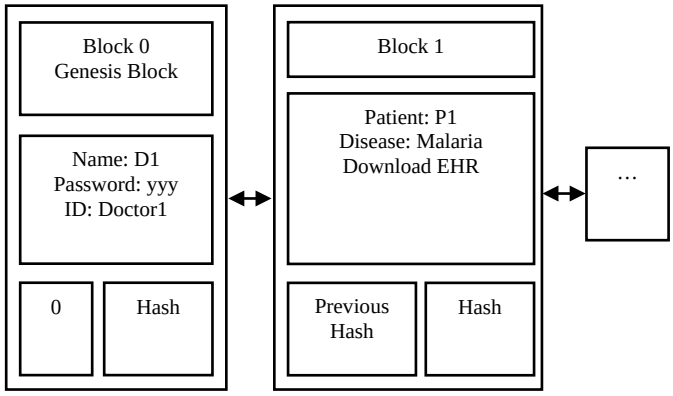

Fig. 6. Doctor Blockchain.

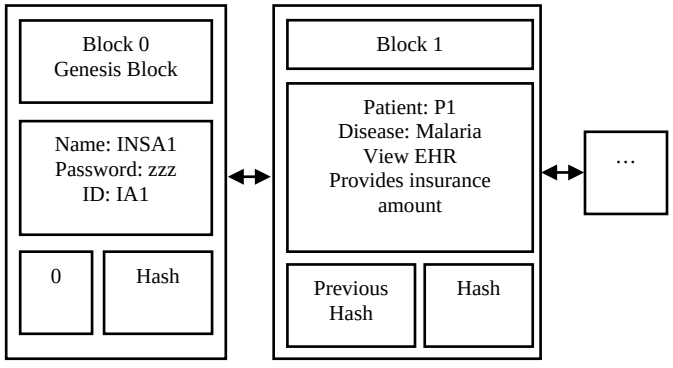

Fig. 7. Insurance Agent Blockchain.

Algorithm-2: Formation and addition of Doctor and Insurance Agent Blockchain

Input: Patient block which is referred from the patient blockchain. Forming Doctor blockchain and adding blocks to it

Output: Forming Insurance Agent blockchain and adding blocks to it

- The doctor and the Insurance Agent downloads the data of the referred patient block to their block with the help of a private key
- Encrypted EHR and Hash with Bilinear Map is retrieved from the block
- Using a private key, decrypt the Encrypted EHR
- The EHR is accessed by the Doctor and the Insurance Agent
- With the help of the Doctor's name, ID and password, create a genesis block for the Doctor similarly create for the Insurance Agent also
- Add the Encrypted EHR and Hash with Bilinear Map to the block
- Add this block to the Doctor blockchain and Insurance Agent blockchain
- The insurance amount for the treatment is transferred to the Patient block.

Algorithm-2 gives the formation and addition of Doctor and Insurance Agent Blockchain. Fig. 6 shows the Doctor Blockchain which consists of a genesis block with the Doctor's name, ID, and password. The information related to the treatment of the diseases was added as a new block one by one. Only the blocks with the patient's permission can be viewed by the doctors. Fig. 7 shows the Insurance Agent Blockchain which consists of a genesis block with the Insurance Agent's name, ID, and password. The information related to the treatment of the diseases was added as a new block one by one. Only the blocks with the patient's permission can be viewed by the insurance agents.

Algorithm-3: Blockchain Validation

Input: Patient Blockchain

Output: Validation Result (Safe or Not Safe)

- Download Patient blockchain
- Status is Safe
- **for** each Block from Blockchain
  - From Block, Encrypted EHR and Hash with Bilinear Map were retrieved
  - Generate new Hash for Encrypted EHR based on HMAC-SHA1 Algorithm
  - Generate new Bilinear Map for Encrypted EHR
- **if** ((Hash == new Hash) & (Bilinear Map == new Bilinear Map)
  - Block = Safe
- **else**
  - Block = Not safe
- **break**
- **end for**

All the data in the EHR were encrypted within the blockchain and cannot be accessed by anyone. The Data Verifier finally verifies the Patient Blockchain, whether it is safe or not. Algorithm 3 gives the steps involved in Blockchain Validation. The block which has to be verified by the data verifier will be searched in the blockchain. Then the Encrypted EHR and the Hash with Bilinear Map will be retrieved based on the HMAC-SHA1 Algorithm, a new Hash for the Encrypted EHR will be generated. Then, if the Hash value is equal to the new Hash value along with the Bilinear Map equal to the new Bilinear Map, the corresponding Block will be considered as Safe Block and if not, then the corresponding Block will be considered as not Safe Block.

IV. Result and Discussion

The access control of the proposed system has been designed in such a way, that the parties like insurance agents and doctors, who were granted permission from the patient can only have the access to the EHR of the patient blockchain so that preventing the access of unauthorized parties to the EHR.

The time consumed for the access of EHR in a blockchain using the proposed approach is compared with existing centralized storage systems and the result has been graphically represented in Fig. 8. Data has been requested to the EHR for accessing and the time is taken to receive the requested data has been noted.

In centralized storage, the EHR will be stored in a centralized server. The patient who needs access to those records should raise an EHR request to the centralized server and this time is noted as T_1. The centralized server, after receiving the EHR request, search for the availability of the particular data and then transmit them to the patient and this time will be noted as T_2. Hence, the time consumed for data retrieval will be calculated using the following formula:

$$Time\ consumtion\ (in\ secs) = T_2 - T_1$$

Moreover, the time consumed for searching and accessing the data would be directly dependent on the size of the EHR. It means the time consumption varies with the size of the EHR, i.e. if the EHR size is small, the time consumed will be less and if the EHR size is large, the time consumed will also be high. The comparison result proves that in centralized storage, the time consumption is higher than that of the proposed blockchain method which has been shown in Fig. 8.

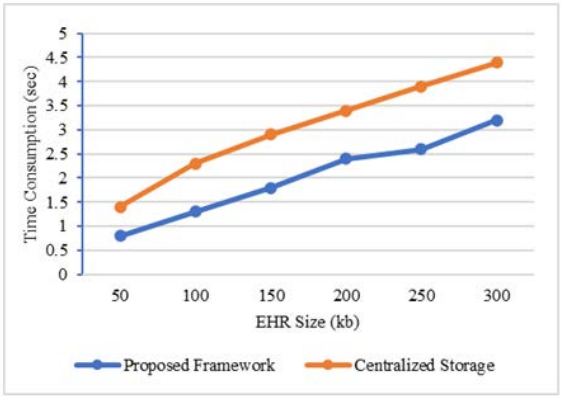

Fig. 8. Comparison of Time Consumption between Centralized Storage and Proposed Framework.

Table I gives the comparison of the features associated with the proposed approach with some existing approaches. The result of the comparison clearly shows that the proposed framework outperforms the existing works and can provide a safe and secure storing and sharing of patient details in EHR using blockchain technology.

TABLE I. Comparison of Proposed Framework with Some Existing Approaches

Feature	[3]	[8]	[9]	[10]	Proposed
Authentication	✓		✓	✓	✓
Identity Management	✓			✓	✓
Decentralized Access		✓	✓	✓	✓
Privacy	✓	✓	✓	✓	✓
Integrity	✓	✓	✓	✓	✓
Availability		✓		✓	✓
Flexibility		✓			✓

V. Conclusion

The proposed framework described the various features of blockchain in the field of healthcare for data storage in EHR and sharing them between the users. This framework overcame the limitations of current data models and supply chains. The access control, time consumption for requesting and searching data in EHR in a blockchain, and the feature comparison were also discussed in this paper and the results show that the proposed system outperforms the existing approaches in all possible ways. From the proposed approach, it is clear that the use of blockchain in healthcare data management prevents data breaches and fraudulent billing and enhances privacy, security, and transparency. Also, data sharing via blockchain facilitates safe and secure sharing among authorized third parties. This approach guarantees secure healthcare management among all the levels which include patients, doctors, hospitals, insurance companies, Pharmaceuticals, etc.

Acknowledgment

The authors would like to thank the Deanship of Scientific Research at Jouf University for supporting this work by Grant Code: (DSR-2021-02-0375).

Funding Statement: This work was funded by the Deanship of Scientific Research at Jouf University under grant No (DSR-2021-02-0375).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Shamshad, S.; Mahmood, K.; Kumari, S.; Chen, C.M. A secure blockchain-based e-health records storage and sharing scheme. J. Inf. Secur. Appl. 2020, 55, 102590.

[2] Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. IEEE Access 2019, 7, 147782–147795.

[3] Ying, Z.;Wei, L.; Li, Q.; Liu, X.; Cui, J. A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access 2018, 6, 53698–53708.

[4] Zibin Zheng; Shaoan Xie et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, 2017 IEEE International Congress on Big Data (BigData Congress), 25-30 June 2017.

[5] E. Bertino, R. Deng, X. Huang and J. Zhou, “Security and privacy of electronic health information systems”, International Journal of Information Security, vol. 14, no. 6, pp. 485-486, 2015.

[6] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records", in 2018 IEEE Globecom Workshops (GC Wkshps), 2019.

[7] V. V., K. Sabarivelan, J. Tamizhselvan, B. Ranjith and V. B., “Utilization of Blockchain in Medical Healthcare Record using Hyperledger Fabric”, International Journal of Research in Advent Technology, Vol.7, No.4, April 2019 E-ISSN: 2321-9637.

[8] Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp. 1–5.

[9] Ramani, V.; Kumar, T.; Bracken, A.; Liyanage, M.; Ylianttila, M. Secure and efficient data accessibility in blockchain-based healthcare systems. In Proceedings of the IEEE Global Communications Conference (Globecom), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 206–212.

[10] Xia, Q.I.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017, 5, 14757–14767.

[11] Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J. Med. Syst. 2018, 42, 152.

[12] Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for secure EHR sharing of mobile cloud-based e-health systems. IEEE Access 2019, 7, 66792–66806.

[13] Ismail, L.; Materwala, H.; Zeadally, S. Lightweight blockchain for healthcare. IEEE Access 2019, 7, 149935–149951.

[14] Cilliers, L. Wearable devices in healthcare: Privacy and information security issues. Health Inf. Manag. J. 2020, 49, 150–156.

[15] Wang, S.; Zhang, D.; Zhang, Y. Blockchain-based personal health records sharing scheme with data integrity verifiable. IEEE Access 2019, 7, 102887–102901.

[16] Linn, L.A.; Martha, B.K. Blockchain for Health Data and Its Potential Use in Health It and Health Care Related Research. In Use of Blockchain for Healthcare

[17] and Research Workshop; ONC/NIST: Gaithersburg, MD, USA, 2016.

[18] Asma Khatoon, A Blockchain-Based Smart Contract System for Healthcare Management. Electronics 2020, 9, 94.

[19] Litchfield, A.T.; Khan, A. A Review of Issues in Healthcare Information Management Systems and Blockchain Solutions; CONF-IRM, 2019.

[20] Kuo, T.T.; Ohno-Machado, L. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv 2018, arXiv:1802.01746.

[21] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” Journal of Medical Systems., vol. 42, no. 7, pp. 130–138, 2018.