Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1535–1551
DOI : 10.47974/JDMSC-1817

Blockchain-based framework for secure and efficient exchange of electronic medical records on mobile cloud environments

Vaibhav Nivrutti Patil *
Vijay H. Kalmani †
Department of Computer Science and Engineering
Jain College of Engineering
Belagavi
Karnataka
India

Abstract

The maintenance of Electronic Medical Records (EMRs) on mobile cloud platforms, in which mobile devices are incorporated with cloud computing to ease healthcare information exchange between healthcare providers and patients, has become a paradigm shift in latest days. This cutting-edge strategy makes it possible to provide medical care at a low overhead expense, with a high level of flexibility, and with electronic health record access. Furthermore, this new approach also expresses concern over the confidentiality of patient data and the safety of the networks that support e-health systems. It is a tough problem to figure out a way to effectively share EMRs amongst mobile users while also maintaining maximum security measures in mobile cloud environments. In this research, a novel framework is presented for the sharing of EMRs that integrates blockchain technology and the decentralized Interplanetary File System (DIFS) on a mobile cloud. The empirical results suggest that the concept offers a useful method for ensuring the reliability of data transfers on mobile clouds, while also preserving important patient data from any potential dangers that may arise. Comparing the results of this performance assessment and security analysis to those of previously implemented data sharing models reveals significant performance enhancements in areas such as lightweight access control method, minimal network latency, maximum security levels, and data privacy protections.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Electronic medical records, Decentralized interplanetary file system, Internet of Things, Blockchain technology.*

* *E-mail:* **vaibhavpatil521@gmail.com (Corresponding Author)**
† *E-mail:* **vijaykalmani@hotmail.com**

1. Introduction

In the healthcare sector, the rise of the Internet of Things (IoT) including wearable technology has brought about a significant increase in the number of possibilities as well as the number of obstacles [28, 29]. The interconnection of smart gadgets creates vast amounts of data pertaining to health. Cloud computing as well as big data analytics can help derive significant and helpful insights from these data outputs, which can then be used to inform more effective decisions. The gathered data may also be used by hospitals and other healthcare organizations so that they might connect with the Electronic Medical Record that is already in existence for the purposes of improved health observation, illness detection, and accurate diagnosis [1]. Furthermore, it may be of use to health insurers in the process of formulating comprehensive strategic programmes for their clients.

It is very important that these kinds of systems have the capability to exchange data in a way that is both effective and safe [4] [5] [6]. Additionally, they are required to offer the particular individuals increased control over access, increased privacy, and increased anonymity. People are going to be unwilling to share their essential information or they are going to avoid seeking medical help when there is no or less privacy, security, and confidence handling [7]. At the moment, the management of sensitive health information in a lot of different information systems is handled by a single entity, which is extremely risky because it creates a singular point of failure. Furthermore, because of the decentralized and distributed nature of blockchains, this dependency may soon be obsolete. It offers the capability to resist failure and assaults in a manner that is both distributed and irreversible.The remaining parts of the paper are divided into the following sections: Section 2 discusses about the research that was done by a number of different investigators. In Section 3, a system model is suggested for the EMRs sharing scheme that makes use of blockchain and smart contracts. Additionally, design goals are stated at this section. In addition, a prototype implementation of decentralized access control for the sharing of EHRs within a mobile cloud blockchain network is demonstrated. In Section 4, the outcomes of the experiments are examined, and Section 5, which contains an evaluation of the system and a security analysis, is presented. In the final section 6, the conclusions are discussed.

2. Review of Literature

An Electronic Health Records (EHR) or Electronic Health Wallet (EHW) system was proposed by Bandar Alamri et. al. [1]. The emerging distributed decentralized t methodologies called as blockchain based HER and EHW has described in details. Both confidential information and interoperability are protected by the GDPR-compliant infrastructure that underpins the EHW's Internet of Things-based Personal Health Record (PHR)technologies. The approach and system design that was proposed include a complete solution for a patient-centered Internet - of - things based PHR system. This approach protects the data privacy of patients and meets the requirements for data interoperability. It is possible to provide medical big data analytics by utilizing the data collected from Internet of Things devices in a manner that does not compromise medical confidentiality if patients are encouraged to submit their data in a managed manner.

Using a data-driven classifier, Heba TakruriTamemiet. al.[2] offer a cost-efficient integrated architecture for storing data related to internet-of-things medical equipment on the blockchain. The classifier that is used in the suggested scheme gets its input from a variety of normal data pertaining to each sort of sensor. A conventional cloud will keep all of a user's data, regardless of whether or not it is abnormal. In order to keep costs to a minimum, the blockchain will only keep records of information that has been deemed aberrant or critical. In addition, an Internet Protocol File System (IPFS) is used with the goal of additional cost reduction. When compared with the conventional method of keeping all data on a blockchain, the expense of preserving healthcare IoT data can be reduced by the proposed methodology by an average of 84%, according to the findings of the experimental investigation.

Yogeshwar et. al. [3] highlights difficulties and issues for BC-based IoT healthcare and provides information regarding the security needs of these domains as a result of typical security procedures. In the context of the Internet of Things, the primary objective of this study is to explore how Blockchain will contribute to an improved healthcare environment. In addition to this, it examines various blockchain-based security solutions, discusses the possibility of using blockchain as a desirable security measure, draws attention to potential issues in the healthcare area, and combines all of these aspects into a single cohesive whole.

P. P. Ray et. al. [4] propose an innovative privacy-preserving strategy that is relied on blockchain as well as swarm exchange methods to enable

the seamless and secure transfer of information of user information (for example, information that relates to electronic medical records) through protected swarm modules of peer-to-peer communications. This scheme was developed in order to facilitate the seamless and safe transfer of information. The GnuPG, IPFS, as well as Golang open-source technologies were used in the development of the scheme that has been presented. The proposed research resembles a number of different kinds of Internet of Things-based health sensor nodes, including things like body temp, pulse rate, as well as oxygen saturation all within the context of a blockchain-based swarm exchange framework. According to the findings, the proposed method is superior to a number of peer strategies in regards of blockchain-IoT, swarm exchange, and EHR transmission.

A blockchain-based medical IoT system was proposed by N. Chauhan et. al. [5] for the purpose of ensuring the safety of electronic medical records. In this approach, the patients' medical records are hashed and encrypted before being saved on the servers of the clinic, and the blockchain is used to record the hash values of the encrypted records. Using the Ethereum blockchain, the major goal is to provide an acceptable, secure, and authorized admission to this vital clinical data pertaining to the patients. This design, which is built on Ethereum, creates the foundation for an intelligent healthcare system that is both flexible and secure. Additionally, it exceeds the techniques that are now in use.

P. P. Ray et. al. [6] propose a data-flow design that blends the Internet of Things with blockchain. This framework, which is referred as IoBHealth, can be utilized for preserving, obtaining, and managing data related to electronic healthcare.

B. Alamri et. al. [7] explored the IAM system design, security needs, and dangers by talking about BC-based approaches in HIoT applications. It provided an overview of the most important components and technologies that are often included in BC-based identity and access management systems, as well as the layered design of the BC-based IAM system found in HIoT. As a result, a summary of the needs and threats to the security was provided. The comprehensive security architecture, hazard identification, and safety and functional performance assessment methods for BC-based IAM in HIoT systems are lacking, according to the findings of the comprehensive study.

B. Mallikarjuna et. al. [8] suggested an integrated strategy of blockchain 4.0 technology utilized in an IoT-based cloud environment. This would minimize the latency while transmitting medical records and incorporate blockchain-based electronic health records known as BEHR.

Propagation of these records would take place among patients and their physicians. The effectiveness of the proposed approach was evaluated and the results demonstrated that the BEHR is a more effective method in regards to response time as well as file transmission and storage of EHR than the existing traditional system is.

M. H. Chinaei et. al. [9] developed a system design that is relied on blockchain and smart contract. This design makes it possible for officials to adaptively avail a verification service for records of a subject machine from a decentralized set of witnesses. These observers are inclined to provide (in a manner that protects their privacy) their local wireless measuring system in exchange for monetary exchange. Thus it, established a model that allows for the best selection of witnesses in such a manner that, subject to the limitations of monetary cost, the verification fault is minimized. Real Wi-Fi session records are acquired from a structure that is comparable of a hospital and has five main stages and more than 30 access points. These traces are then used to evaluate the effectiveness of the suggested solution. The current pricing plan of the Ethereum public blockchain indicates that the strategy makes it possible for healthcare officials to authenticate transmitted data from a traditional wearable device with a validation defect of the order 0.01% at an expense of less than $ 2 for a 1-hour witnessing service. This is accomplished at an expense of less than $ 2 per hour.

M. R. Bataineh et. al. [10] suggests an IoT-Blockchain framework that makes use of an Ethereum Framework together within rich-thin client IoT methodology. The purpose of this architecture is to address the issues that are caused by the limited IoT resources that arise when attempting to develop the Blockchain mining method in IoT systems. The distribution of the load over the available resources is essential to the architecture. Thin-clients are devices with limited resources, while rich-clients are devices with higher resource capacities. Both clients have access to the blockchain and can collect data from it, but the rich-client is the only one that can mine the crypto currency.

A. S. Pallivalappil et. al. [11] present a way for maintaining secrecy for block chains and the internet of things by combining the benefits of cloud computing and blockchain technology. This technique combines IoT and provides IoT services to block chain nodes. Meanwhile, it accumulates, evaluates, and functions on identity verification for health data, and it saves this data in the block chain. Interaction and addressing the insufficient computing capacity of certain block chain nodes is necessary to certify the accuracy of the information and the ability of the project. The simulation

experiment demonstrates that the proposed method is effective, which supports this assertion.

Z. Zulkifl et. al. [12] proposes a behavior driven adaptive security measure for health - care IoTs and networks depending on blockchain by utilizing fuzzy logic. It has presented a heuristic algorithm towards behavior driven adaptive security offering AAA services. The purpose of implementing FBASHI is to investigate both the system's safety and its usability. In addition, a comparison is conducted with the other approaches that are dependent on blockchain technology.

Attribute-based encryption is essential for the Internet of Things; say Naregal K. and Kalmani V. in [13]. The study reveals potential issues with implementing ABE for cloud-based IoT applications and suggests approaches to resolving them. The cloud is a multipurpose platform that may be used for a wide range of tasks like data storage, application development, and server management. Due to ABE's ability to grant or deny access to very tiny data sets, it has become a popular encryption method for use in cloud-based services. The usage of Internet of Things (IoT) devices and cloud-based apps has both grown rapidly in the recent decade, as their respective user bases have shown. Due to the cloud's abundance of storage space and computing power, it is expected that many IoT devices would utilize the cloud to store their data.

The most efficient routing and clustering protocol in WSN, developed by Prakash K. S. and Vijay Kalmani, uses a hop-by-hop energy-saving scheme [14]. In research focus on energy efficncy in secure distributed WSN. Improved network coupling between nodes makes this protocol the best choice for clustering and routing in WSNs. The variables of network stability, network longevity, and the selection of a cluster monitor method are all studied and improved by our proposed updated technique. If you want to save the most power possible, you should probably merge your sensors' outputs. The simulation results showed that the suggested protocol greatly improved network characteristics, making it a potentially useful alternative for WSNs. Threats to WSNs may be reduced thanks to detection and key management approaches developed by Vijay H. Kalmani and others [15].

Nana Yaw Duodu et. al. [16] proposed a system electronic Health record management using IoT and various machine learning techniques. Using Internet of Things (IoT) technology, this platform will gather health data from students in their dorms, then utilize machine learning to forecast students' health state using their EHR data from the school. Using a sophisticated Wireless Body Area System to deploy with IoT sensors and

cameras, students will be able to report their health concerns to school officials.

Rita Roi et. al. [17] describes utilization of blockchain in supply chain management. The purpose of this research was to analyses the level of blockchain technology adoption in the Indian food supply chain. This research tried to use blockchain technology to investigate the tracing of food items along the food supply chain. Those in the food industry who are interested in tracing and tracking techniques may find this research useful. The outcome is encouraging for the use of blockchain technology in the forest products sector. Additionally, it provided a springboard for the implementation of blockchain technology in FSC businesses for the purpose of achieving operational excellence. This research demonstrates that FSC industries may improve their business processes and supply chain integrity by using blockchain technology.

Farah A. Abdulghani et. al. [18] Arabic text classification according to mutual information using deep learning techniques. In this study, we concentrated on English text but also conducted some preliminary tests with Arabic language. There are many stages involved in text classification, beginning with document preparation (by the stop word and stem approach) and ending with extraction of features and classification. Using complementary data in a hybrid advanced machine learning model for categorizing, a novel method was presented for classifying Arabic text.

Basim A. Hasan et. al. [19] conjugate gradient method for eliminate the optimization problems. Nonlinear conjugate gradient methods that priorities objective function data are provided in this study. a variety of examples of numbers, one of the strategies is just as effective as the status quo, if not more so.

3. Research Methodology

In a mobile cloud platform, an electronic-health case is investigated, in which patient data are collected from a collection of local gateways utilizing Internet of Things and maintained on a public cloud for the goal of sharing with healthcare providers.

Process of Blockchain

Hash Generation: The process of transforming an initial piece of data into a digest, also known as a hash, is referred to as hashing. The message is converted in an irreversible manner due to the employment of cryptographic hash algorithms in the procedure. The message is subjected

to the hash function, which then produces a message digest in the form of a hexadecimal output of a predetermined size.It accepts inputs of any size and may deliver messages of any length. The Message constitutes INPUT N. It encrypts the message by means of a cryptographic hash function, which we'll refer to as H.The result is produced which is referred to as Digest.***H(N) = Digest****Hash* functions cannot be reversed in any way. This indicates that it is a one-way function, and utilizing the digest to recreate the original message is not possible.Determinism can be used to hash functions. It never produces a different hash when using the same input data, maintaining consistency. The hash, on the other hand, is extremely sensitive to even the smallest of letter changes. The example of hash generation is;

N: Bye → SHA-256(N) → 165D8DB22271FF25F561A5FC928B1E24.

Take note of the dissimilarities between the two messages' outputs. In addition, even a little modification to the function or the message can cause the digest to undergo considerable transformations. The Avalanche effect is the name given to this particular characteristic. In the system that we have developed, the most well-known hashing algorithm, known as SHA-256, is used. The subsequent section delves into the specifics of this method in greater detail.

Mining on a blockchain is the procedure of calculating a new block to be uploaded to a distributed ledger [8]. Mining is also known as "cryptocurrency mining." Computers used for mining are typically very powerful devices because they are responsible for creating the right hash values. The nodes that are participating in the mining process are tasked with resolving a mathematical conundrum by utilizing their mining equipment. The network is informed when a miner has successfully produced a new block as soon as the miner has successfully produced the block. The mining of that block is halted, and each miner in the channel begins the process of resolving the computations for the following block again. A miner will take the value of the hash and add it to the nonce at some point throughout the mining procedure.

Consensus

In a democratic setting, the members of a network can be kept in sync with the help of something called a consensus algorithm. When a network is decentralized, every member of the network possesses an equal amount of power to make choices within the system. Therefore, in order for network members (also known as nodes) to make new modifications

to the system in accordance with a global consensus, rules need to be developed. The operation of a decentralized network can be accomplished using a variety of consensus procedures. Every methodology has its own method for achieving a worldwide consensus on a modification to a network's configuration. In the system that we have suggested, we have incorporated a proof of work algorithm.

Proof of work (PoW) – It is a mechanism for reaching consensus that is utilized by the Bit coin network (Nakamoto, 2008). In order to authenticate oneself via POW, a sophisticated computational technique is required. In the proof-of-work protocol, every node in the network is responsible for determining a hash value for the ever-evolving block header. The value that is computed must either be identical to or less than a particular given value, as this is a requirement of the consensus. In the decentralized network, every participant is required to constantly compute the hash value by employing a variety of nonces until the goal is accomplished.

When one node acquires the pertinent value, all of the other nodes are obligated to independently validate the value to ensure it is accurate. In the event that there were fraudulent transactions, the subsequent transactions with in new block will be validated. After that, the group of transactions that was utilized for the computations is accepted to be the authenticated outcome, which is represented by a new block being added to the blockchain. Miners are the nodes that perform the POW method of calculating hashes, and the mining process itself is known as mining.

Smart Contract - The smart contract is the portion of the blockchain that has been defined, and it is this section that acts as the access point to the blocks, transactions, and background of the blockchain. The smart contract's underlying computer code can be found in the decentralized database. The business logic is carried out by the smart contract, which also adds limitations and validates transactions, among other things. The addition of information, the performance of operations, and the presence of contracts are all dependent on smart contracts. In order to facilitate the exchange of EHRs, a cloud-based blockchain network is being built. Because of its many benefits, a platform based on Ethereum was chosen. The following is a description of the primary components that make up the cloud blockchain network.

Data uploading and sharing on proposed mobile blockchain

Utilizing smart contracts as well as blockchain technology allows for the introduction of two methods that facilitate the uploading and

sharing of data in a secure manner. The utilization of smart contracts enables the automatic management of transactions and processes on blockchains, resulting in increased productivity and dependability. Specifically, a blockchain client component will be built to be installed on every mobile device. This module will execute the full functionality required for participating in a cloud blockchain network. This module is in charge for encoding transactions and information requests, digitally signing transactions, and connecting to blockchains for the purpose of tracking transactions. In addition, the user interface component is created for user interaction, as well as a request handler component is developed for the purpose of processing data regarding user requests. Figure 2 is an illustration of the work flow for the operations of uploading and EMRs. The following is a short summary of the explanation of each event.

1. In order to begin a new transaction for transferring data to a cloud server, a mobile gateway must first initiate the request.
2. The blockchain client handles the processing of the request and then transmits it for validation to the EMRs management and the smart contracts.
3. The request is validated by the manager of EMRs using smart contracts in accordance with a stringent control policy. In the event that the request is granted, a reply will be sent back to the gateway, which can then be used to upload data.
4. The gateway may now select EMRs, which is a healthcare information file received from wearable sensors, and encrypt the data using the public key of the EMRs manager. After that, the gateway sends the encrypted document to the cloud storage location used by DIFS.
5. The DIFS storage will save the data file into a relevant storage node utilizing uploading data (AreaID, PatientID), and it will immediately return a hash value that will be preserved in the DHT table. Using this information, the DIFS storage will save the data file.
6. Uploading transactions are combined together into data blocks, which are then entered into the transaction pool for validation by miners so that they may be appended to the blockchain. The uploading transaction is modified at the mobile gateway so that it can be tracked.
7. The mobile user must first join the blockchain network before preparing a transaction including request information (requestIDs)

and signing it with the private key SK in order to obtain data stored in the cloud.

8. The user establishes a connection with the cloud and utilises the blockchain client module to transmit a data access request to the cloud.
9. The EMRs manager will validate the user's access right using the access control approach that incorporates smart contracts. The EMRs management will perform an analysis of the requestIDs as soon as the access request has been validated, and then they will send this data to the DIFS storage in order to get the data.
10. The EMRs manager uses an asymmetric encryption technique to decrypt the information requested, and then sends the decrypted data to the person who made the request for the data.
11. The patient's mobile device, which is being used for monitoring via the blockchain client, receives an update regarding the transaction that is being uploaded:

4. Algorithm Design

Algorithm I: Initialization of generation of hash for transactional data

Input: input the textual data as Transactional_Data[]
Output: Gen_hash for input textual data
Steps

1. Choose the Transactional_Data[]
2. On Transactional_Data[], Apply the SHA-256 algo
3. Gen_hash= SHA-256(Transactional_Data[])
4. Final hash for input data as Gen_hash

Algorithm II: Peer to Peer verification protocol in m nodes

Input: client input query as textual data Cur_Node[A_Ch], other silent nodes Nodes_Ch[VMNode_id] and [VMNode_Ch]

Output: In the event that the current cannot validate the chain, automated recovery of the blockchain will occur.

Steps

1. Data, either in the form of transactions or events that is inputted into the blockchain.

2. Retreivalblockchain of current server for duration [d_duration]
   VMCur_ACh, VMCur_node[ACh]
3. for each

$$NodesCh\ [Nodeid,Ch]\sum_{i=1}^{m}(GetCh)$$

   End for
4. for each (j into VMNode_ACh)
   If (!equalsVMNodeACh[j] to (Current_ACh))
   Flag_Value = 1
   else
   continue transaction;
   to the other nodes, store the data
5. if (Flag_Value == 1)
   BnodeCnt = SimOfNodesBlockch()
6. Carry out the evaluation using the algorithm for majority voting.
   Recover the entirety of the chain based on the data from all servers.
7. end if,
   end for,
   end for

Algorithm III. Hash generation by Transaction Mining Technique

Input:SCnt[] Smart contract, CHT[]Current hash Transactions, PHash[] Previous hash

Output: Valid hash generation

Steps

1. Generation of hash_Val for the lth transaction
2. If (Generated_hash_Val is as per to Defined_SCnt [])
   Commit the generated current hash
   Flag_Value =1
   Otherwise
   Flag_Value=0
   Continue with next cycle
3. Execute till flag_Value = 1
   Return valid_hash[]

5. Discussion and Conclusion

When several access requests are being processed simultaneously, the average amount of time that cloud computing consumes is measured. When compared with the system that does not require authentication process, the methodology that uses smart contracts for user authentication takes substantially more time to execute user requests. This overhead results from the amount of time spent authenticating users' identities and accessing resources. Furthermore, even in the most extreme case situation, where there are seven requests, the additional cost is still just approximately 100 milliseconds, which is regarded to be tolerable in real-world scenarios because it is still minimal. This outcome indicates that the proposed model's identity verification and access control system may be designed with a minimal amount of programming.

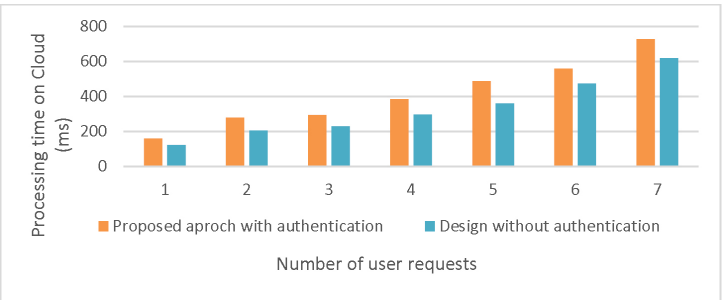

Figure 1

Time overheads for processing time on cloud versus user requests

The Figure 1 shows time for proposed method for sharing EMRs is also assessed in regards to the amount of communication overhead associated with accessing EMRs stored on blockchain cloud storage DIFS. The total amount of time required for the EMRs access procedure, originating with the request for data access and ending with the data being received on the mobile phone, is the amount of time that is measured. When compared with centralized storage, the time overhead associated with retrieving EMRs from the proposed blockchain-based storage DIFS is examined. The results of the experiments reveal that the suggested decentralized storage scheme on blockchain surpasses the traditional scheme with centralized storage in regards to the amount of time that is required for overhead. This finding also suggests that the proposed EMRs distribution on the cloud blockchain is an efficient use of resources.

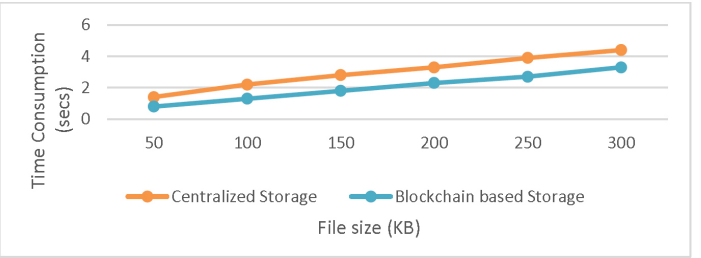

Figure 2

Time overheads in terms of time consumption for EMRs access on cloud storage

The network latency evaluation makes it abundantly clear that the suggested design is capable of achieving a lightweight EMRs distribution with the minimal amount of system overheads in contrast to the traditional cloud design. The proposed data sharing system is analyzed and evaluated using a variety of performance indicators in order to illustrate that it is feasible to implement the suggested model in actual usability settings.

6. Conclusion and Future Work

The proposed novel method of exchanging EHRs be implemented, one that is supported by mobile cloud computing and blockchain technology. The most significant problems with the existing systems for sharing electronic medical records are identified, and effective alternatives to overcome these problems are suggested, all of which are shown using a working prototype. The work that is proposed focuses on building a reliable access-control system that is based upon a specific smart contract in order to regulate user contact for the purpose of guaranteeing that the transmission of EMRs is both safe and effective. For the purpose of achieving decentralized data storage and data exchange, the peer-to-peer DIFS storage system has been merged with blockchain technology. The results of the implementation reveal that the proposed methodology can, in contrast to existing methods, make it possible for users in the healthcare profession to share medical data across mobile cloud environments in a safe and expedient manner. The security analysis and detailed assessments are presented on many technological aspects of the proposed approach, demonstrating the benefits of the suggested solution in comparison to other options that are currently available. It is considered, that blockchain

enabled system provides effective data management for electronic health records. For the future enhancement to collaborate the system some deep learning algorithms for classification and role based access control for authorization based security will be much effective in distributed manner.

References

[1] B. Alamri, I. T. Javed and T. Margaria, "A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain," 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-5 (2021), doi: 10.1109/NTMS49979.2021.9432661.

[2] H. T. Tamemi, M. Rabayah, K. A. Raad, M. Kanaan and A. Awad, "A Low Cost Blockchain-Based Framework for Preserving Critical Data in Health-Care IoT Systems Using Classification," 2022 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-8 (2022), doi: 10.1109/DSC54232.2022.9888800.

[3] Yogeshwar A. and S. Kamalakkannan, "Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1-9 (2021), doi: 10.1109/ICICCS51141.2021.9432198.

[4] P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," in *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857-10872 (1 July1, 2021), doi: 10.1109/JIOT.2021.3050703.

[5] N. Chauhan and R. K. Dwivedi, "A Secure Design of the Healthcare IoT System using Blockchain Technology," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 704-709 (2022), doi: 10.23919/INDIACom54597.2022.9763187.

[6] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in *IEEE Systems Journal*, vol. 15, no. 1, pp. 85-94 (March 2021), doi: 10.1109/JSYST.2020.2963840.

[7] B. Alamri, K. Crowley and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review,"

in IEEE Access, vol. 10, pp. 59612-59629 (2022), doi: 10.1109/ACCESS.2022.3180367.

[8] B. Mallikarjuna, D. Kiranmayee, V. Saritha and P. V. Krishna, "Development of Efficient E-Health Records Using IoT and Blockchain Technology," ICC 2021 - IEEE International Conference on Communications (2021), pp. 1-7, doi: 10.1109/ICC42927.2021.9500390.

[9] M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," in *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10117-10130 (15 June15, 2021), doi: 10.1109/JIOT.2021.3051433.

[10] M. R. Bataineh, W. Mardini, Y. M. Khamayseh and M. M. B. Yassein, "Novel and Secure Blockchain Framework for Health Applications in IoT," in IEEE Access, vol. 10, pp. 14914-14926 (2022), doi: 10.1109/ACCESS.2022.3147795.

[11] AS Pallivalappil, S. S. Ahmad, Y. Raju, C. K. Kumar, T. M. W and N. Krishnaiah, "Applications of Ensuring Security and Privacy Using Block Chain with IoT for Health Record," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1911-1917, (2022) doi: 10.1109/ICACITE53722.2022.9823735.

[12] Z. Zulkifl et. al., "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," in IEEE Access, vol. 10, pp. 15644-15656 (2022), doi: 10.1109/ACCESS.2022.3149046.

[13] Naregal K, Kalmani V. Study of lightweight ABE for cloud based IoT. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 134-137 (2020 Oct 7). IEEE.

[14] Sonwalkar PK, Kalmani V. Energy Efficient Hop-by-Hop Retransmission and Congestion Mitigation of an Optimum Routing and Clustering Protocol for WSNs. *International Journal of Advanced Computer Science and Applications*. 13(3) (2022).

[15] Kalmani VH, Alias SS, Jogadand RM, Rai HM. An Efficient Key Management Scheme with Key Agreement to Mitigate Malicious Attacks for Wireless Mesh Network. *International Journal of Computer Applications*. 56(6) (2012 Jan 1).

[16] Duodu NY, Patel W. Advanced EHR system in homes-in-schools' automation using internet of things and machine learning. *Journal of Information and Optimization Sciences*. 43(8) : 1953-62 (2022 Nov 17).

[17] Roy R, Chekuri K, Sandhya G, Pal SK, Mukherjee S, Marada N. Exploring the blockchain for sustainable food supply chain. *Journal of Information and Optimization Sciences*. 43(7) : 1835-47 (2022 Oct 3).

[18] Abdulghani FA, Abdullah NA. Hybrid deep learning model for Arabic text classification based on mutual information. *Journal of Information and Optimization Sciences*. 43(8) : 1901-8 (2022 Nov 17).

[19] Hassan BA, Abdullah ZM, Hussein SA. A new family of conjugate gradient methods to solve unconstrained optimization problems. *Journal of Information and Optimization Sciences*. 43(4) : 811-20 (2022 May 19).