Hindawi
Security and Communication Networks
Volume 2022, Article ID 4645585, 10 pages
https://doi.org/10.1155/2022/4645585

Research Article

Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment

Sanjeev Kumar Dwivedi,[1] **Ruhul Amin**,[1] **Jegatha Deborah Lazarus**,[2] **and Vijayakumar Pandi**[2]

[1]*Department of Computer Science & Engineering, DR SPM International Institute of Information Technology (IIIT-NR), Atal Nagar-Nava Raipur, Chattisgarh, India*
[2]*Department of Computer Science & Engineering, University College of Engineering Tindivanam, Tindivanam, India*

Correspondence should be addressed to Jegatha Deborah Lazarus; blessedjeny@gmail.com

Received 6 May 2022; Accepted 29 July 2022; Published 15 September 2022

Academic Editor: Jie Cui

The blockchain is a peer-to-peer distributed ledger technology that works on the precept of "write-once-read-only." In a blockchain, pieces of information are arranged in the form of blocks, and these blocks are linked together using the hash value of previous blocks. The blocks in a blockchain mechanism are appended only, which means that once information is stored in a block and it cannot be changed; no one tampers the block's content. The traditional electronic medical records (EMRs) based system stores the patients' information in a local database or server, which provides centralization of information, and traditional EMRs are more centric on the health providers. So, security and sharing of patients' information are difficult tasks in the traditional EMR system. The blockchain mechanism has the potential to resolve these existing problems. Due to the appended-only-ledger principle and decentralization of blocks between the network participants, blockchain technology is suited to the EMR system. In this article, first, we discuss all the existing EMR systems and discuss their drawbacks. Keeping all the drawbacks in our mind, we propose a blockchain-based medical record system that utilizes clouding technology for storage purposes. Furthermore, we have designed a smart contract and consensus algorithm for our proposed EMR. Our system only uses a permissioned blockchain model so that only verified and authenticated users can generate their data and participate in the data-sharing system.

1. Introduction

In the recent epoch, patients' medical information is growing rapidly due to the collaboration of information technology (wearable Internet of things devices, e.g., wearable sensors) and the healthcare system. The patients' medical information is important because it provides significant help for medical researchers as well as service providers to turn up with the proper result, which will help to diagnose patients [1]. Medical researchers and service providers often want to share patients' data. So securely storing the patient data is a crucial task [2]. The traditional electronic medical record-based (EMR) system does this task. The EMR-based system provides real-time patient records, ease of access to these records, improved accuracy, sharing of patient data between different researchers, and safety and security to the patient data compared to the paper-based system [3]. In the paper-based system, maintaining and storing patient data is a difficult task (such as huge numbers of rooms are needed to store patients' records, etc.), and the safety of records is also not guaranteed [4, 5]. Malicious users are easily able to do harmful activity in these records. To rectify these problems, the electronic medical record-based system is used in comparison to the paper-based system. But still, in the traditional EMRs-based system, many pitfalls are present.

1.1. Shortcoming of Existing Electronic Medical Record (EMR)-Based Systems. Currently, electronic medical records (EMRs)-based systems are widely popular because they can manage the huge volume of patients' data and provide easy access to these data. But although, there are several drawbacks present in the existing EMRs-based system.

(i) The EMRs-based system stores data related to a patient in a local database or server, which provides centralization to the patients' data [6]. If users or service providers want to access the patients' data, they directly access it without the patient's intervention.

(ii) The traditional EMRs-based systems are more centric on health providers. The health providers (i.e., hospitals, authorities, etc.) share the patient's data without the patient's knowledge. Therefore, they can manipulate the data. As a result, the originality and integrity of data are at high risk.

(iii) The records of the patients are not secure and safe in the traditional EMRs-based system. Malicious users (or) attackers enter the EMR system due to the lack of security and privacy mechanism [7, 8] present in these systems, and then they tamper (or access) the patient's data.

(iv) The sharing of patients' data in the traditional EMRs-based system becomes problematic because different health providers use different encryption methods and schemas [9]. (even if the patient has agreed to share the data with service providers).

(v) Currently, IoT-based smart devices [4, 10, 11] (i.e., wearable sensors) are also generating the patient's data. Generally, cloud servers (such as storage) are used to store patient's data [12, 13]. But, this mechanism demands more cost and time in maintenance. Therefore, the system's overall efficiency has degraded [14, 15].

(vi) Due to the health providers' centric approach, they can modify the patients' data. So updating the medical records in the EMR system is also a big challenge.

In summary, the current EMR system has several pitfalls, such as centralized storage and inadequate access control mechanism. Therefore, a decentralized technique is highly required to store the patient's data, and at the same time, it should provide privacy and security, proper access control mechanisms [16], and authenticity for the patients' data [7, 17, 18]. The blockchain mechanism can solve the problems mentioned earlier. Due to its inherent characteristics, it is well suited to healthcare applications [4, 5, 14, 15].

1.2. Motivation behind the Proposed Work. Many pitfalls exist in the traditional electronic medical records (EMRs) system, which motivated us to propose a new framework for the EMR system using blockchain technology. A few of them are discussed here.

(i) In the traditional EMR system, patients' data is stored in the central database, and in a centralization system, the "single-point-failure" problem exists. This existing problem motivates us to design a new system in which patients' data is stored in a decentralized way such that if any node fails, then also we will be able to retrieve the patient's data. The blockchain mechanism is well suited for the abovementioned problem.

(ii) In the traditional EMR system, the security and privacy of patients' data in vulnerable. The present system does not provide a sufficient solution for these problems. With the integration of blockchain technology in the current EMR system, patient data security and privacy can be achieved.

(iii) The traditional EMR systems are more centric on health providers. They share the patients' data without the knowledge of patients. To rectify this problem, a suitable system is needed where patients are the central authority for sharing their medical data with other providers.

(iv) In the traditional EMR system, health providers cannot share the patient's data, even if patients concur to share their data. The reason behind this problem is that health providers use different schemas to store the data in their local databases.

So, a proper mechanism is needed which can resolve all these problems. Blockchain technology has the potential to resolve all these problems.

1.3. Major Contributions. This article presents the following contributions:

(i) We have rigorously performed the literature review for the blockchain-based electronic medical health record system and then we have also discussed the shortcomings of the existing system.

(ii) A proposed framework for an electronic medical health record system with blockchain technology has been proposed by considering all aspects of the EMR system.

(iii) We have designed a smart contract algorithm using a finite state machine for the proposed EMR system.

(iv) We have also designed a consensus algorithm for the proposed EMR system.

(v) Finally, we have given some future research challenges with security concerns.

1.4. Organization of the Article. The rest of the article is organized as follows: the literature review for the EMR system is presented in Section 2. Section 3 deals with the proposed architecture with smart contract and consensus algorithm, followed by concluding remarks for the article in Section 4.

2. Related Works

Many authors attempted to solve the problems of the traditional EMRs based system by using the blockchain mechanism [4, 5, 19, 20]. Some authors also used the smart contracts mechanism to solve it. Uddin et al. [4] proposed “A Patient Agent (PA) Based Remote Patient Monitoring (RPM) Architecture.” Every patient has its own patient agent in their architecture, which is stored on the patient local server (PLS). In their architecture, PA selects one node as a miner among the available nodes, and the miner’s work is to generate a hash value of the current block. Xia et al. [5] proposed a blockchain-based data-sharing scheme. The framework proposed by Xia et al. addresses the problem associated with sensitive data stored in the cloud environment. The authors suggest the patient-centric solution in [12] for health data sharing system, using a private blockchain. Azaria et al. [19] proposed a MedRec: a decentralized record management system to handle electronic medical records using blockchain technology. The problem with the proposed architecture is the security of the individual database. They did not address this problem, and the key management problem remains unsolved in the proposed architecture. Chen et al. [20] proposed a new business process for medical information sharing based on a blockchain mechanism. The proposed approach is “patient-centric,” where patients are the central authority for viewing and sharing their medical records. The limitation of this method is the smart contract mechanism.

Yang and Li [7] proposed a blockchain-based architecture for EHRs systems, using a new incentive mechanism to create a new block. The architecture works on top of the existing database, which healthcare provider maintains. Griggs et al. . [13] proposed blockchain-based smart contracts to secure remote patient monitoring. The proposed framework uses a private (permissioned) blockchain. Al Omar et al. [8] proposed a permissioned blockchain-based healthcare data management system to attain privacy and security. The proposed solution is a “Patient-Centric” approach in which the patient is the sole authority to keep the data on a blockchain. Dubovitskaya et al. [9] proposed a blockchain-based healthcare data management framework, especially for electronic medical records (EMRs) systems. They provide a secure and trustable framework for sharing in the EMR system. Novikov et al. [21] presented a decentralized blockchain-based infrastructure to store patients’ electronic medical records (EMRs) in a healthcare system.

Table 1 compares the existing blockchain-based medical records system concerning blockchain taxonomy (i.e., smart contracts, consensus algorithm, authentication, key management, and 51% attacks, etc.). In Table 1, two abbreviations are used: ND and PB. In this specific column, PB means the type of blockchain is permissioned blockchain, and ND means that the authors did not discuss the type of blockchain. The solution provided by the authors is applicable for both permissioned and permissionless blockchains. ND means that the respective authors did not discuss the corresponding blockchain taxonomy in other columns. Table 2 compares the existing approach with its advantage and disadvantage.

3. Proposed Architectures

3.1. System Overview. Our proposed architecture comprises the following components (or entities): a central authority and a management system, known as CAMS, a list of the service provider (e.g., doctors, insurance companies, and research organizations, etc.), the user (generally, a patient), a pool of Data Lake, hash generators, and a cloud server. These entities are connected using a decentralized peer-to-peer architecture. The architecture of the proposed system is shown in Figure 1.

3.2. Role and Responsibilities of the Involved Entities

(i) Central Authority and Management System (CAMS): the CAMS is responsible for generating a pair of keys and issuing the same keys using the cryptographic mechanism to the user and service provider. The proposed framework utilizes the permissioned blockchain system. If any new user or service provider wishes to join the system, firstly, they take permission from CAMS. Here permission means that the CAMS authenticate them because the new user or service provider may be a malicious user. CAMS is also responsible for managing the entire system. CAMS has a list of users and service providers who are already present in the network. If any new user or service provider joins, then after the process of key generation and authentication, CAMS updates the list, which tells that currently how many users and service providers exist in the system.

(ii) User: the user is generally a patient who wants services from service providers. All users have a copy of smart contracts which tells about the agreement or set of protocols—the copy of smart contracts issued by the CAMS. If any user wishes for services from service providers, this request is checked by smart contracts. If smart contracts are executed correctly, then, only the user can take the services from service providers; otherwise, not. The service providers are doctors, hospital authorities, insurance claim companies, and medical researchers, etc.

(iii) Service providers: service providers provide their services to the user according to the need of the user. Service providers are doctors, insurance companies, laboratory offices, and scientific researchers, etc. The user consults with a doctor for specific medical treatment. The doctor gives suggestions accordingly. Doctors often suggest a specific medical test according to the user’s problem. For this, the user goes to the laboratory office (inside or outside the hospital) to perform the test. If the laboratory office gives the result immediately to the patient, then the patient shows these results to the doctor and gets suggestions for some medicine, if required.

Table 1: The comparison of existing approaches with their advantages and disadvantages.

Researcher	Blockchain	Type smart contract mechanism	Consensus algorithm	Authentication and key management	Scalability	Mining incentive	Blockchain specific vulnerability
Uddin [4]	ND	No	No	No	ND	Yes	ND
Xia [5]	PB	No	No	Yes	Yes	No	ND
Liang [12]	PB	No	No	No	No	No	ND
Azaria [19]	ND	Yes	Yes	No	ND	Yes	ND
Chen [20]	PB	No	Yes	Yes	Yes	No	ND
Yang [7]	ND	Yes	No	No	Yes	Yes	ND
Griggs [13]	PB	Yes	Yes	No	ND	ND	ND
Al Omar [8]	PB	Yes	No	Auth.	ND	ND	ND
Dubovitskaya [9]	PB	No	Yes	Yes	No	No	ND
Novikov [21]	ND	Yes	No	Auth.	ND	ND	ND

ND: not discussed; PB: permissioned blockchain; Auth.: authentication; No: not present or did not discuss the required algorithm or mechanism; and yes : provided required algorithm or mechanism.

Table 2: The comparison of existing approaches with their advantages and disadvantages.

Reference	The idea of the article	Advantages	Disadvantages
[4]	A patient agent (PA) based remote patient monitoring (RPM) architecture.	The PA selects miners based on the available CPU resources and previous performance of miners. So by doing this time is minimized.	The smart contract mechanism and consensus mechanism are not discussed in this article. This architecture is also vulnerable to denial of service attacks and ransom cyber-attack.
[20]	A new business process for medical information sharing based on a blockchain mechanism.	The proposed approach is "patient-centric" where the patient has all the authority for viewing and sharing his/her medical records.	The authors do not investigate and analyze the smart contracts mechanism under the permissioned blockchain.
[7]	A blockchain-based architecture for EHR systems using a new incentive mechanism for the creation of any new block in a blockchain-based system has been proposed.	The proposed architecture uses a smart contract mechanism for agreement between patient and provider.	The proposed architecture is a "provider-centric" approach.
[13]	A blockchain-based smart contract for secure remote patient monitoring has been discussed.	The proposed method uses smart contracts and the PBFT consensus mechanism.	Key management and authentication and blockchain-based specific vulnerability (51% attacks) part are not discussed by the author.
[21]	A decentralized blockchain-based infrastructure for storing the electronic medical records (EMR) of the patients in a health care system.	This scheme uses a patient-centric model with the support of smart contracts to access patient data.	The consensus mechanism and blockchain-related vulnerability are not discussed by the author.
[5]	A blockchain-based data sharing scheme.	The proposed architecture is scalable to any number of nodes.	The communication and authentication protocols are not discussed.
[12]	A solution for health data sharing using a private blockchain has been discussed.	The method proposed is a patient-centric approach.	The authors do not explore the underlying smart contract and consensus mechanism.
[8]	A permissioned blockchain-based healthcare data management system to attain privacy and security for healthcare data has been proposed.	The proposed solution is a "patient-centric" approach. Smart contracts are helpful for interaction with the blockchain.	They assume that the user is having a key and password. How these keys are generated, they did not discuss.
[9]	A blockchain-based healthcare data management especially for electronic medical records (EMR) has been proposed. The proposed framework consists of the membership service, local database, cloud server, chain code, and the user (either patient or doctor) and nodes with his own ledger. Practical byzantine fault tolerance (PBFT) for the consensus mechanism has been used.	This scheme supports access control and data availability with desired security.	The issue with the framework is scalability. Blockchain-based specific vulnerability (51% attack) is not discussed by the author.
[19]	MedRec: a decentralized record management system, to handle electronic medical record systems by using blockchain technology has been proposed.	In this architecture, they used smart contracts.	The problem with the proposed architecture is the security of an individual database.

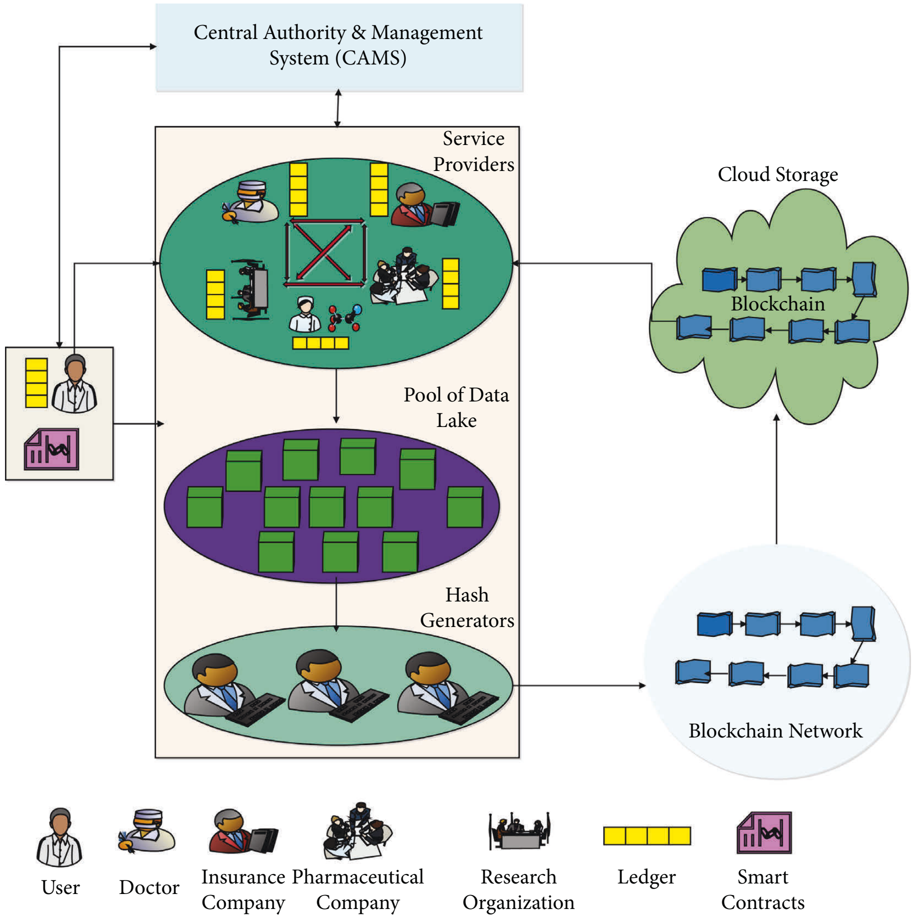

Figure 1: Proposed architecture.

Sometimes laboratory office directly gives the result to the doctor. Many users also take insurance plans like health insurance plans and term insurance plans according to their needs; therefore, insurance companies have also come into the picture as service providers. Pharmaceutical companies interact with doctors and insurance companies to brand and sell their medicine. Scientific researchers interact with different service providers (doctors, pharmaceutical companies, and users) for their research. Due to all these activities, a huge volume of data is generated. The EMRs system without a blockchain cannot handle this (as discussed in section 1). But by using the blockchain with EMRs system, trust in a patient's data increases and transparency of the entire system

(iv) Pool of data lake: the pool of Data Lake contains the bunch of data that users and service providers generate. Service provider gives their services (a patient consults a doctor and provides description of health records and insurance records) to the user; and all these huge amounts of data are kept inside the pool of Data Lake. The pool of Data Lake is a container (or database) used only to store the generated data.

(v) Hash generators: the hash generators generate the hash value of the current block. The hash generators module takes the data from a pool of Data Lake and converts it into the size of a specified block. First, they validate the block. After the validation process, they keep the block inside the blockchain system. CAMS specifies the size of the block. In the proposed system, more than one hash generators exist. The CAMS module picks the suitable hash generator, depending on the existing performance of hash generators. So at any point in time, only one or two online hash generators are available.

(vi) Cloud server: the cloud server only stores the blocks in the blockchain network. Our proposed architecture uses the cloud server instead of a local database because the volume of data is high. As per the discussion in section 2, these blocks are connected by using the hash value of previous blocks, so tampering with the data in any block is impossible. If scientific researchers want to use the patient's data for research purposes, they can use it with the user's permission only. Without the user's permission, scientific researchers, as well as service providers, are not able to take and share the user's data. Since the user data are stored in the blockchain system, using the cryptographic mechanism, it provides security for tamper-proof and immutable of user data.

3.3. Algorithm for the Proposed System. The algorithm for the proposed system is as follows:

(i) *Step 1.* CAMS authenticates the user who wants services from the service provider.

(ii) *Step 2.* If the user's authentication is successful, then the user is granted to take services from providers; otherwise, the error message is generated: authentication is not successful.

(iii) *Step 3.* If a new user wants to join the system, the new user may join after CAMS approval. The CAMS generates the pair of keys, and steps 1 and 2 are repeated.

(iv) *Step 4.* The user consults with service providers, and the data generated by them are kept in a pool of Data Lake.

(v) *Step 5.* The hash generators collect the data from the Data Lake pool, verify it, convert it into a block, and add it to a blockchain by using the previous block's hash value. This step is repeated after a while.

(vi) *Step 6.* Steps 4 and 5 are repeated for every user who wants services from the provider.

(vii) *Step 7.* Finally, the blockchain is stored in a cloud server.

3.4. Smart Contract Algorithm of the Proposed System. As per discussion, in Figure 2 in section 2.6, smart contracts are based on the state machine model, and the state machine model is always a deterministic state machine model. Smart contracts are define the set of rules, which are written in the form of the program (or scripts). This set of scripts are stored on all the nodes of the blockchain system. In turn, the blockchain nodes execute these scripts to perform certain activities or transactions in the network [22, 23]. By using the same concept, we also propose a deterministic state machine model for the proposed system since a deterministic state machine model is represented as a directed graph, and a directed graph consists of a set of vertices and a set of edges. In the deterministic state machine model, these sets of vertices are referred to as a set of states, and a set of edges is referred to as a transition from one state to another state or in the same state. The advantage of showing the smart contracts using the state machine model is that it is very easy for the developer to write the code by seeing the flow of the state machine. Moreover, it triggers the events to achieve the necessary behavior, which suits the EMR system. Furthermore, disclosing the smart contract code to external parties is not required. They can predict the system behavior and write the code with add-on requirements. Our proposed state machine consists of 4 states: labeled as state 0, state 1, state 2, and state 3. The user is represented as state 0; CAMS is represented as state 1; service providers are represented as state 2. State 3 is called a dead state. The proposed state machine model is shown in Figure 2.

In the state machine model, certain actions are defined: Authentication, No Action, Violation, and Permission. This set of actions is used to transition from one state to another. For example, if the machine is in state 0 and the action is Authentication, then the machine automatically moves from state 0 to state 1. If the machine is in state 1 and the action is Violation, then the machine automatically moves from state 1 to state 2. If the machine is in state 2 and the action is No Action, then the state does not change and so on (see Algorithm 1).

The solidity programming language can be used to implement the proposed smart contract for the EMR system. It is a statically-typed programming language influenced by other languages such as JavaScript, C++, and Python. Moreover, this language is designed to run on the Ethereum Virtual Machine (EVM). The Remix IDE with the solidity version 0.5.10 is used to execute the suggested smart contract. Remix IDE provides a convenient platform to deploy smart contracts. It provides three different environments (JavaScript VM, Injected Web3, and Web3 Provider) to execute and deploy smart contracts [24]. Furthermore, the execution cost plays a crucial role when smart contracts are executed in any of these three environments. Execution cost determines the total cost (in terms of "gas") required to execute the defined computational operations.

3.5. Consensus Mechanism for Proposed System. The consensus algorithm is the set of rules to reach a common viewpoint or agreement. The consensus algorithm is designed so that, after executing the block, all the nodes (or majority of nodes) in a network agree that the block is valid and can be included in the blockchain network. Once the agreement is done, no node can change the decision. For the proposed system, we also designed a consensus mechanism for the verification and validation of a new block [25]. In our proposed architecture, a new block is verified and validated with the help of hash generators. The main work of hash generators is to validate the block (whether the correct user sends the block or data or not because it may be possible that malicious users send the data in a pool of data lake, so validation is needed) and after the validation of new block, generate the hash value of new block, and finally add them in a blockchain.

In the proposed architecture, more than one hash generator exists but only one hash generator is responsible for validating and generating the hash value of the new block. The work of other hash generators is to validate the new block. The selection of hash generators is based on the previous performance of the hash generators or on the stake or wealth deployed in the network because the service providers also act as hash generators. The reason behind this is if the service providers act as a hash generator, based on their wealth deployed in a system, then the chance of malicious activity is very less because in that case, if they are performing a malicious activity, they are damaging their own wealth. In the proposed system, two categories of hash generators exist. In the first category, only one hash generator exists which is responsible for both validating as well as generating the hash value of the new block, and in the second category, remaining hash generators exist which are responsible for validating the new block only (see Algorithm 2).

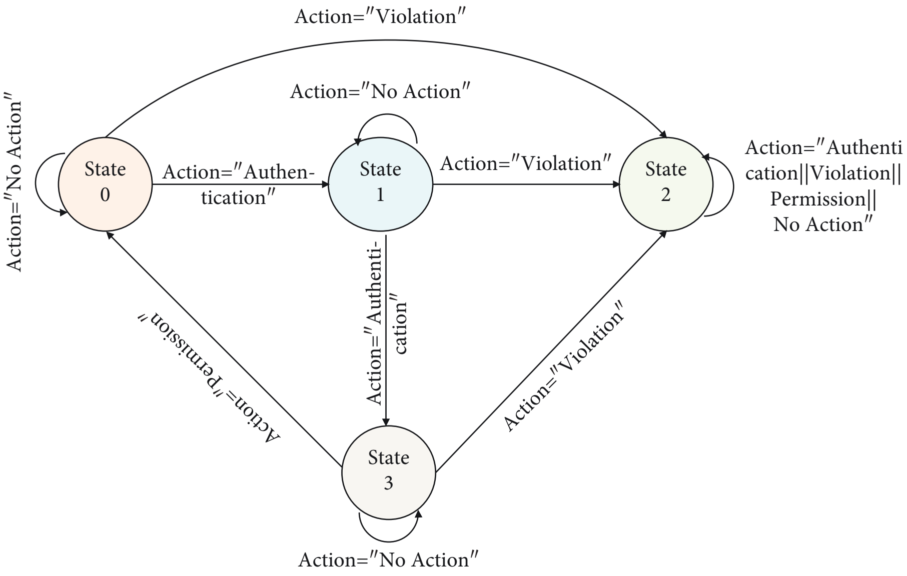

Figure 2: Smart contract using a finite state machine.

```
Require: Actions such as Authentication, Violation, Permission, No Action
Ensure: Messages such as Authentication successful, Error and abort, Permission granted, No Action required
FOR STATE 0 AND STATE 1:Action: Authentication, violation, No action
If (f(Action) = = Authentication) then
    f(Message) = authentication is successful;
    move: S (1)
    ← S(0);
Else if (f(Action) = = No Action) then
    f(Message) = No action required;
    move: S (0)
    ← S(0);
Else if (f(Action) = = Violation) then
    f(Message) = error and abort;;
    move: S (3)
    ← S(0);
End if
FOR STATE 2:Action: Permission, violation, No action.
If (f(Action) = = Permission) then
    f(Message) = take permission;
    move: S (1)
    ← S(2);
Else if (f(Action) = = No Action) then
    f(Message) = No action required;
    move: S (2)
    ← S(2);
Else if (f(Action) = = Violation) then
    f(Message) = error and abort;
    move: S (3)
    ← S(2);
End if
FOR STATE 3:Action: Permission, authentication, violation, No action
If (f(Action) = = Permission/Authentication/Violation/No Action) then
    f(Message) = error and abort;
    move: S (3)
    ← S(3);
End if
```

Algorithm 1: Smart contracts as state machine model.

```
Require: Authentication value, Validation value, Genesis block
Ensure: New block, Blockchain length, Nonce-value SP[n] = list of service providers; HG[] = hash generators; Per[] = performance
    for hash generators; BCl = block chain length;
    $A_v$ = authenticating value provided by hash generators; $V_v$ = validating value provided by hash generators; BC: Blockchain; B0:
    Genesis block;
$A_v = 0$;
$V_v = 0$;
$BCl = 1$;
$Per = 0$;
For ($i = 0$ to hash_generator − 1) do
    Execute Per[HG[i]];
End for
Per ← Per[HG[0]];
For ($i = 1$ to hash_generator) do
    If ($Per[HG[i]]\&gt;Per$) then
        Per ← Per[HG[i]];
    End if
End for
Display: Selected hash_generator)
For ($i = 0$ to hash_generator − 1) do
    Check authentication of selected hash_generator;
    If (Authentication == true) then
        $A_v = A_v + 1$;
    End if
End for
If ($A_v \geq \lceil HG[m]/2 \rceil$) then
    Display: Authentication is successful;
End if
Create a new block by using the selected hash_generator
For ($i = 0$ to hash_generator − 1) do
    Check validation of new_block by all hash_generators;
    If (Validation == true) then
        $V_v = V_v + 1$;
    End if
End for
If ($V_v \geq \lfloor HG[m]/2 + 1 \rfloor$) then
    Display: Validation is successful;
End if
While (TRUE) do
    Calculate the Proof_Hash value for new_block;
    If (Proof_Hash == Target_Value) then
        $BCl = BCl + 1$;
    End if
    Change Nonce_value;
End while
```

Algorithm 2: A consensus algorithm for proposed architecture

3.5.1. Consensus Mechanism of the Proposed System

(1) In the first phase, after the selection of the hash generator, the remaining hash generators first authenticate this selected hash generator. If [ceiling (N/2)] number of hash generators authenticates this selected hash generator (assume that in a system "N" number of hash generators exist, excluding the selected one), then authentication is successful and it proceeds further; otherwise, the system aborts it with a message: authentication not successful; error message.

(2) In the second phase, the selected hash generator picks the data from the pool of Data Lake, converts it into a block, and sends the new block to other hash generators for validation. All the hash generators, including the selected one, validate the new block. If [floor (N/2) +1] number of hash generators, validate the new block (assume that in a system "N" number of hash generators exist, excluding selected one, +1 is used for selected hash generator) then validation of a new block is successful and it proceeds further, otherwise, the system aborts it with a message: validation not successful; error message.

(3) In the third phase, the selected hash generator generates the hash value of the new block and is added to the blockchain system.

4. Conclusion

In this article, we present the blockchain-based novel approach for electronic medical records (EMRs) systems. The proposed blockchain-based system provides several advantages compared to traditional electronic medical records-based systems. Traditional EMRs systems are more centric on healthcare providers. Whereas the proposed BMRS approach is centric on the patient only, which means that if the healthcare providers want to access the patient's data, they can access and share the patient's data with the patient's permission, which is an advantage over the traditional EMRs system. In the proposed architecture, hash generators are responsible for the maintenance of the blockchain system, including the creation of a new block, validation of a new block, and finally, adding the block to the blockchain network. The service providers also act as hash generators. The proposed system considers both smart contracts mechanism as well as a consensus mechanism. The smart contracts mechanism is based on the state machine modal. Hash generators use the consensus algorithm to authenticate the healthcare providers and to validate new blocks.

In future work, our research team will try to incorporate the incentive mechanism with its mathematical model and provide a solution for the mitigation of various attacks, such as routing attacks and phishing attacks that increase the security of the EMR system.

Data Availability

The datasets generated or analyzed during the current study are not publicly available because the data are strictly confidential because the manuscript is based on patient records that are maintained electronically. The authors understand that these data are to be maintained confidentially and hence they are not provided in the manuscript or elsewhere.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Review on "Blockchain technology based medical healthcare system with privacy issues"," *Security and Privacy*, vol. 2, no. 5, p. e83, 2019.

[2] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.

[3] P. T. S. Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," in *Information and Communications Security. ICICS 2016*, K. Y. Lam, C. H. Chi, and S. Qing, Eds., Springer, Berlin, Germany, pp. 254–261, 2016.

[4] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patient Agent to manage blockchains for remote patient monitoring," *Studies in Health Technology and Informatics*, vol. 254, pp. 105–115, 2018.

[5] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[6] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *Proceedings of the 2016 ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, ML, USA, August 2016.

[7] G. Yang and C. Li, "A design of blockchain-based architecture for the security of electronic health record (EHR) systems," in *Proceedings of the 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 261–265, Nicosia Cyprus, December 2018.

[8] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science*, G. Wang, M. Atiquzzaman, Z. Yan, and K. K. Choo, Eds., Springer, Berlin, Germany, pp. 534–543, 2017.

[9] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing Using Blockchain," in *Proceedings of the 2017. AMIA Annu Symp Proc American Medical Informatics Association*, Washington, DC, USA, November 2017.

[10] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[11] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: a literature review," in *Proceedings of the IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, pp. 763–768, Ohrid, Macedonia, July 2017.

[12] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "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)*, Montreal, QC, Canada, October 2017.

[13] 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, p. 130, 2018.

[14] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, UAE, November 2017.

[15] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, May 2017.

[16] J. P. Dias, L. Reis, H. S. Ferreira, and Â Martins, "Blockchain for Access Control in E-Health Scenarios," 2018, https://arxiv.org/abs/1805.12267.

[17] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in *Proceedings of the 2016 Smart City Security and Privacy Workshop (SCSP-W)*, April 2016.

[18] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[19] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: using blockchain for medical data access and permission

management," in *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, August 2016.

[20] J. Chen, X. Ma, M. Du, and Z. Wang, "A blockchain application for medical information sharing," in *Proceedings of the 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE)*, April 2018.

[21] S. P. Novikov, O. D. Kazakov, N. A. Kulagina, and N. Y. Azarenko, "Blockchain and smart contracts in a decentralized health infrastructure," in *Proceedings of the 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, September 2018.

[22] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *Journal of Information Security and Applications*, vol. 54, Article ID 102554, 2020.

[23] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain-based secured IPFS-enable event storage technique with authentication protocol in VANET," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1913–1922, 2021.

[24] S. K. Dwivedi, M. S. Obaidat, R. Amin, and S. Vollala, "Decentralized management of online user reviews with immutability using IPFS and Ethereum blockchain," in *Proceedings of the 2022 International Mobile and Embedded Technology Conference (MECON)*, March 2022.

[25] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey," *Security And Communication Networks*, vol. 2021, Article ID 7142048, 21 pages, 2021.