Journal of Computer Science

Original Research Paper

Smart Patient Consent Management Model for Health Information Exchange Based on Blockchain Technology

K. R. Rohini, P. S. Rajakumar and S. Geetha

Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamilnadu, India

Article history
Received: 15-02-2024
Revised: 18-03-2024
Accepted: 27-03-2024

Corresponding Author:
K. R. Rohini
Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamilnadu, India
Email: gsmnaidu@gmail.com

Abstract: Innovation for Electronic Medical Records (EMRs) has been hindered by years of excessive regulation and inefficient bureaucracy. As data science and personalization encourage individuals to take an active role in their healthcare and regain control of their own medical records, there is an urgent need for new approaches. The ability to exchange electronic health records is fundamental in contemporary healthcare systems for facilitating a wider range of health services and delivering high-quality treatment. Despite the requirement for utilizing medical information for various reasons, most patients still authorize paper forms with minimal participation. The present methods of managing patient consent and medical data exchange are laborious, expensive, and prone to failures, even with quality assurance measures in effect. Because of this, there may not be enough patient empowerment, which can lead to inefficiencies in the process and a lack of trust and transparency. A shortage of resources makes it harder to acquire individual consent, which is necessary for health data exchange. Healthcare organizations also grapple with patient consent. Blockchain-based platforms enable data exchange by developing a trusted user network. Users can share their data without relying on health service providers for time and resources. Blockchain-based systems necessitate data governance frameworks to specify and monitor data exchange and use. This research article aims to establish a system that healthcare organizations may use to easily gain patient consent for various objectives, while also giving patients more flexibility in managing their consent. In this study, a novel electronic consent model namely 'Smart Consent Blockchain Based System (SCBCS)", is built on the hyper ledger fabric Blockchain that employs a purpose-based access control method. Distributed ledger technology (blockchain) ensures that all metadata pertaining to patient records, permissions, and data access cannot be altered once written. Additionally, Blockchain chain code is developed to handle patient consent-related business logic. A prototype is constructed and verified business logic with the chain code, validating the requestor's data access and patient permission saved in the Blockchain. The proposed SCBCS acts as a consent management system for patients and healthcare organizations. The proposed method is compared with other existing methods 'MedRec', Consent Management System (CMS). The results demonstrate this system manages medical staff data access requests effectively. The proposed method outperforms other methods compared with low latency, less gas consumption, and low access time. This Blockchain-based proposed SCBCS technology offers great dependability, transparency, and traceability for patient data sharing in hospitals and research.

Keywords: Healthcare, Electronic Health Records, Patient Medical Data, Patient Consent Management, Purpose Based Consent, Blockchain, Hyper Ledger Fabric

Science Publications

Introduction

Electronic Health Records (EHR) are shared between patients and healthcare professionals through a procedure called Health Information Exchange (HIE). Fewer readmissions, fewer prescription errors, better diagnoses, and less repeat testing are just a few of the potential healthcare benefits of timely HIE. Digital transformation has been a game-changer for every sector in the past decade and it's engulfing the healthcare industry at the moment.

The transmission and storage of patient records is now more efficient. Patients would experience less hassle and more efficiency as they can be easily shared among institutions that use Electronic Health Record (EHR) systems to record patient visits. By gathering patients' permission, healthcare providers can aggregate their data into massive amounts of information, which will allow them to make analyses and provide personalized treatment. Research in the fields of medicine and pharmaceuticals is also anticipated to benefit from it. Nevertheless, obtaining patient consent is necessary prior to sharing and using patient data.

A number of systems have been developed specifically for HIE, such as Regional Health Information Organizations (RHIOs) and Community Health Management Information Systems (CHMIS) (Vest and Gamm, 2010). Low clinical efficiency, patient privacy risks, data insecurity, insufficient integration of different data sources, and reliance on central data storage are some of the ongoing issues with HIE. The latter problem, in certain cases, has led to persistent animosity between rival service providers. The high expense of running and maintaining these systems is another obstacle. Patients are unable to take advantage of HIE when they go to hospitals outside of their home systems because most systems are built for healthcare providers and patients do not have personal access to their data. In addition to the health information exchange, patient consent is another important challenge in a smart healthcare system. Effective health information exchange strongly relies on patients' consent.

In the context of medical records, "consent" (CIOMS, 2016) means that patients are giving permission for third parties to view their medical records. Additionally, "informed consent" (World Medical Association, 2013) is the patient's voluntary assent prior to receiving medical treatment in the context of interactions between healthcare professionals and patients. Whatever the situation may be, obtaining a patient's permission has always been done by having them sign a paper form (usually 3-5 pages long). Patients are wary about signing papers and sharing their data with others because their decisions are difficult to reverse once submitted. The success of a clinical trial depends on the interdependencies among several relevant parties, including trial issues, clinical sites, ethical committees, regulators, and trial sponsors. Most importantly, there must be no compromise on the rights, safety, or welfare of trial participants (ICH E6(R1), 2016; World Medical Association, 2018). Ethical human subject research relies on informed consent, which enables participants to voluntarily engage in a study once they are informed about the trial's purpose, trial flow, benefits, and hazards. Trust and comfort of trial participants are crucial because they affect recruitment, protocol adherence, and study completion, among other things. By signing an informed consent form, trial participants show their trust in the experiment and their readiness to take part.

In response to the aforementioned issue, numerous forms of electronic consent (e-consent) (Coiera and Clarke, 2004; Wuyts *et al*., 2011) have been developed, enabling patients to electronically provide consent using digital signatures and then revoke it if needed. The majority of electronic consent models have relied on a centralized architecture. A small number of these models have also included trusted third-party delegation in their evaluation and assurance of patient permission (Asghar and Russello, 2012). Decentralized blockchain technology is another alternative (Benchoufi and Ravaud, 2017; Rantos *et al*., 2019). One of these projects, the Dwarna initiative (Mamo *et al*., 2020), connects biobank project members through a well-designed web portal for dynamic consent that uses the blockchain ledger. Blockchain technology can be used for effective electronic health information exchange and patent consent.

Distributed ledger technology, or Blockchain, ensures that all user transactions are always up-to-date. Every user inside the blockchain has the ability to openly audit all transactions. The data is immutable once a transaction has taken place. Data's intended use is determined by its purpose information in Byun and colleagues' relational database model (Byun and Li, 2008; Byun *et al*., 2005).

An organization's well-known Role-Based Access Control (RBAC) model is the foundation of their proposed solution. This model assigns data access permissions to functional roles inside the hierarchy. In subsequent work, Kabir *et al*. (2011) proposed conditional purpose-based access restriction for dynamic roles, which greatly enhanced the model. In this context, a new approach is proposed in this article to address the issues of successful health information exchange and effective patient consent using blockchain technology.

The proposed system “Smart Consent Block Chain based System” (SCBCS), includes the feature of purpose-based access control, a key component of data access control models that limits the use of patients' data to what they had originally intended.

The proposed system SCBCS employs a block blockchain-based, entirely decentralized e-consent system, which uses an RBAC-inspired purpose-based access control approach. The proposed system gives patients greater flexibility in how they give their consent. Assigning a specific purpose to each piece of data allows patients to manage their consent specifically and healthcare organizations and research institutions can obtain patient records for future needs based on patients' consents. These two main contributions help manage patient consent across different organizations.

To provide a safe channel in a network involving participating healthcare organizations, the proposed system SCBCS employs Hyper Ledger Fabric (HLF), a consortium Blockchain platform (Androulaki *et al*., 2018; Hyperledger, 2020). While Electronic Health Records (EHRs) store patient records off-chain, the blockchain's ledger includes patient consent, record addresses, metadata, and hash values. On the other hand, it is possible to save the patient's consent off-chain in addition to their medical records. By comparing the hash value on the blockchain with that of the received one, data integrity is preserved and malicious change of data on the blockchain is almost impossible. This article provides a novel approach compared to the existing approaches. The major features of the proposed SCBCS are:

1. Uses a decentralized blockchain system for patient e-consent
2. Uses purpose-based consent management
3. Uses hyper Ledger Fabric (HLF), a consortium Blockchain platform for effective health information exchange
4. Uses hash values to secure patients' consent and medical records
5. Grants access only based on the purpose of the data intended

Although it is not an easy process, numerous academic efforts have been directed towards creating appropriate protocols for privacy and security in the healthcare system using blockchain technology, particularly with consent management (Stanley, 2021).

Kosba *et al.* (2016) suggest moving health records from different databases to one main database by utilizing the conventional database storage system and the mobile agent paradigm. With an emphasis on data pre-processing and data transformation, (Lin and Liao, 2017) present an architecture for healthcare big data management and analysis. Centralizing health data storage is typically accomplished through the use of a cloud-based system, as the associated costs and technical support requirements are quite significant. Data theft, corruption, integrity, authentication, and privacy violations are among the many security issues they face.

Data exchange, data access management, and medical history maintenance are just a few of the possible blockchain uses in healthcare that Watanabe *et al.* (2016) mentioned. In order to put blockchains into practice, the authors stress the need for smart contracts and express worry over scalability in the context of application development. By investigating the scalability of health data-sharing smart contracts, we find a straightforward solution to this issue.

The problem of consent-based data sharing in genomics is discussed by Riggs *et al.* (2019). In order to avoid lengthy agreement terms, they propose a web-based consent form that is only one page long for sharing genetic data. Using a survey with 5,162 participants, they demonstrated that the streamlined consent form leads to better data access.

Most notably, hyper ledger Fabric (Androulaki *et al*., 2018) is the foundation for the consent-based double-blind anonymous data exchange proposed by Bhaskaran *et al.* (2018). Their approach specifies the components of a permissioned blockchain-based Know Your Customer (KYC) application. In contrast to our solution, this strategy does not work well in a permissionless environment where everyone can sign up for the platform and start making contributions.

Two blockchain-based methods for checking the accountability of data provenance are ProvChain (Liang *et al*., 2017) and DataProv (Ramachandran and Kantarcioglu, 2017).

Modeling dynamic consent is not the primary focus of these strategies, though. An approach to data accountability and provenance monitoring is proposed by Neisse *et al.* (2017) using blockchain technology. With the permission of data suppliers, their technology permits data tracking and reuse. A smart contract outlining the solution's terms of use and data provenance information is included in the package.

The utilization of blockchain technologies for permission management has been recently proven by Zyskind and Nathan. By storing encrypted data and recording pointers on the blockchain, they establish a reliable blind escrow service (Zyskind and Nathan, 2015).

For hypothetical key management in a healthcare setting, Kish suggested the Blockchain (Kish and Topol, 2015). Users are able to configure their preferred level of privacy for the Internet of Things devices they engage with using the framework suggested by Cha *et al.* (2018). A central gateway handles all communications and verifies that the data sent is in line with the user's choices. To further guarantee that no sensitive data has been accessed without the user's agreement, blockchain technology is used to both secure and manage the privacy choices that each user has chosen. However, the framework fails to take into account the requirements of GDPR and the crucial interaction with data controllers when it comes to obtaining consent.

A semi-autonomous context-aware agent makes decisions in the user's place in the work described in Copigneaux (2014). The agent decides what to do depending on context, behavior, and a reputation system that is community-based. Although the system gives the user control, there's a chance it won't pick the right privacy settings for things that don't fit the pattern of activity it's been tracking.

Additionally, Cha *et al.* (2017) suggest using Blockchain gateways, with a configuration optimized for Internet of Things (IoT) applications and, more especially, for usage with legacy devices. Specifically, users can save time and effort by connecting to many blockchain-enabled gateways with a single account, rather than registering for each individual gateway. These gateways act as intermediaries, processing requests and responses from devices in the correct order.

Neisse *et al.* (2016), see an alternative method for delivering informed consent. Users can have a clear idea of how the system will use their personal data with the proposed framework. However, this particular technology is exclusively intended for use with cooperative intelligent transport systems. The data access and usage policies are defined in advance by the data owners, who use a policy-based approach.

Zhuang *et al.* (2018), several healthcare process scenarios were simulated using programmed smart contract laws. The purpose of this proof-of-concept study is to simulate possible methods for the persistent monitoring of clinical trials across various census regions. A suite of customizable smart contract settings has been developed to utilize various degrees of data access privileges. These parameters mimic the procedures used by the entities responsible for monitoring, the trial and clinical sponsors' sponsors, and the subjects themselves.

Zhuang *et al.* (2019), present a blockchain paradigm that integrates various trial-based contracts for managing trials and involving patients, as well as a master smart contract for automating subject matching, recruiting patients, and managing trial-based contracts.

Aldred *et al.* (2019) detail the planning and execution of a feasible decision-capable permission-based Blockchain third-party consent management system. In order to demonstrate the viability of the service, which gives users agency over their data management decisions, the authors built a proof of concept implementation on hyper ledger Fabric. In their opinion, the suggested approach satisfies the requirements of the General Data Protection Regulation (GDPR) of the European Union. The solution adheres to the seven privacy design criteria policies.

The immutable versioning control and integrity of personal data processing consents are safeguarded by a blockchain infrastructure. Lastly, the paper showcases a working prototype of the platform that is being suggested, which enables the primary functionality of consent administration.

The article presented by Rantos *et al.* (2019), showcases a working prototype of the platform that is being suggested, which enables the primary functionality of consent administration.

The immutable versioning control and integrity of personal data processing consents are safeguarded by a blockchain infrastructure.

Using hyper ledger fabric, Dara in Tith *et al.* (2020), provides a new model of electronic consent that is implemented by a blockchain system and makes use of a purpose-based access control method. Blockchain technology ensures that all metadata pertaining to patient records, consents, and data access may be exchanged among participating organizations in an immutable manner.

Azaria *et al.* (2016), present MedRec, an innovative blockchain-based decentralized record management system for electronic medical records. In addition to providing patients with convenient access to their medical records across physicians and treatment sites, our technology also provides them with a complete and immutable record. Important considerations when dealing with sensitive information include authentication, secrecy, accountability, and data exchange; MedRec handles all of these by utilizing unique blockchain capabilities. However, it fails to recognize modification of patient data.

All the above studies concentrate on patient consent for the usage of medical records for various purposes. They are not dealing with efficient ways of usage of medical records, in particular, for the intended purpose. All the methods reviewed fail to recognize the false transaction related to medical records.

The proposed method SCBCS in this article, constructs a safe route in a network amongst participating healthcare organizations by utilizing a consortium Blockchain technology, Hyper Ledger Fabric (HLF) (Zhang *et al.*, 2019). The blockchain's ledger includes the patient's consent, the record's address, metadata, and hash values, but the actual records of the patient are kept off-chain in the appropriate electronic health records. The patient's permission, however, can also be kept off-chain with the patient's records. To ensure data integrity, the blockchain compares the hash value with the received one, making malicious changes to the data almost impossible.

Materials and Methods

Here, the proposed model's data request process is detailed and how this proposed patient consent model adapts the purpose-based access control scheme is discussed. A quick overview of blockchain and HLF is forecasted before moving on to the idea and implementation of the proposed system. The proposed model SCBCS consists of the following modules:

1. Consent purpose
2. Consent model
3. Access request
4. Blockchain framework
5. Chain code

Consent Purpose of the Patient

The rationale for collecting and using data is called a purpose (Byun and Li, 2008). It is the most important part of a patient's consent since it shows that the patient wants their data used only for a certain purpose. That is, purpose can be both broad and specific and it can be structured hierarchically in a "purpose tree," as illustrated in Fig. 1. The purpose tree used in this proposed approach as given in the below figure consists of education, medical treatment, and insurance fields. Further, they are classified into survey, statistics, discovery, diagnosis, report, documentation, and claim. With the broadest reach, the general purpose is at the very top of the tree, with its descendant purpose nodes below it. In the purpose tree, each line connecting two nodes stands for a relationship between them. Organizations share the same objective in exchanging data and the purpose-tree shows that. Due to the strong relationship between the purpose tree and the privacy policy, it is essential that all member organizations reach a consensus on its structure and attributes.

The "intended purpose" is the data's related goal, which is to control who may access it, and the "access purpose" is why people want to get to the data in the first place. A patient's consent form will often outline the intended objective, which is to say, the reason why the data can be accessed. Therefore, it is important for the requestor to specify the purpose of data access when making a request. This reason should be compared to the data's intended use as stated in the patient's agreement. In cases where the two goals are congruent, the system grants access to the requested data. The consent model establishes the matching rule by outlining the ways in which a requestor prescribes an access request with the access purpose and how the patient agreement identifies the intended purpose. If a patient selects "medical_treatment" as the data access's intended purpose in a general consent model, then the system will only grant access to requestors whose access purpose matches "medical_treatment" or any of its descendants in the purpose tree. As seen in Algorithm 1, the purpose tree from Fig. 1 is now stored in the blockchain as a JSON array type.

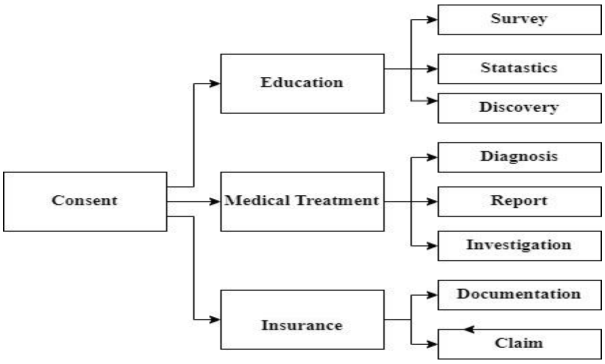


Fig. 1: Consent tree hierarchy

Algorithm 1:

Algorithm (Consent Purpose):

```
“Consent”: {
     “Education”: {
              “Survey”: {}
               “Statistics”: {}
              “Discovery”: {}
       },
      “Medical_Treatment”: {
          “Diagnosis”: {}
          “Report” “{}
          “Investigation”: {}
       },
        “Insurance”: {
          “Claim”: {}
          “Documentation”: {}
       }
}
```

Consent Model

When a patient agrees to the use of their data, it is only for the purpose that was mentioned in the above section. Furthermore, patients typically grant varying degrees of authorization to healthcare providers based on their roles. A role is defined in the RBAC model's role hierarchy and stands for an organization's job function or title (Nakamoto, 2016). The job title determines the level of access privilege. Data owners can more easily grant access to data based on the role of the requestor instead of identifying the user in the organization.

The consent model of the proposed method SCBCS is created based on modifying the RBAC concept and the purpose-based access control method. In the proposed concept, the patient's consent specifies the data access purpose and the role of the individual user. This approach to job hierarchy is in favor of an approach that is both straightforward and easily understood by all parties involved. Patients can prepare a list of data consents to reply to different requests for data access.

The patient consent list is created by combining various consents with different responsibilities and goals. Requests for access to data are approved if they match one of the consents listed. A basic illustration is shown in Algorithm 2. Our method stores consent along with the appropriate patient records' metadata and hash value in a blockchain. On the other hand, it can coexist with patient records held off-chain. Every consent is made up of four primary fields, which are represented as follows.

The sample consent is given below:

$$< Role, Id, Action, Specific\ Purpose >$$

where:
Role : Job position of the requestor
Example : Nurse, Doctor
Id : Identity of the requestor provided at their workplace
Action : 'Read' and 'copy'
The copy includes the read action also but not vice versa permitted
Specific Purpose: For which the requestor wants to read/copy the patient data, as mentioned in Fig. 1

Algorithm 2:

Algorithm (Consent Role):

```
"Consent": {
"Patient ID": #1
{
        "Role" = Doctor
          "ID" = 01
          "Action" = Read/Copy
          "Specific Purpose" = <Consent – Medical
        Treatment – Diagnosis
},
{
           "Role" = Doctor
           "ID" = 02
           "Action" = Read/Copy
           "Specific Purpose" = <Consent – Medical
        Treatment – Investigation
},
{
             "Role" = Nurse
             "ID" = 01
             "Action" = Read
             "Specific Purpose" = <Consent – Medical
        Treatment – Report
}
```

Access Request

Proper qualification and a valid purpose must be stated by the requestor when requesting access to data. Access to the chosen data activity is granted once the requestor's role and purpose for access have been satisfactorily authenticated.

Actually, in order to access some patient records, the requestor must include the necessary keywords and the access request in a data search query. Medical history, demographics, time and date, hospital, department, physician, illness, and other patient-related terms are among the data elements and keywords. The process begins with the acquisition of the target list and continues with the validation of each candidate's access request against the patient's permission.

Out of the four primary tuples involved in patient consent in the proposed model, the requestor's job and eID are typically fixed, as they are recorded in their respective systems or organizations. Aside from the access purpose and action, the only variables in the access request are these. First, the system verifies the requestor's identity using the eID. Then, it checks the requestor's function in relation to the patient's permission. If needed, it can consult with the participating organizations.

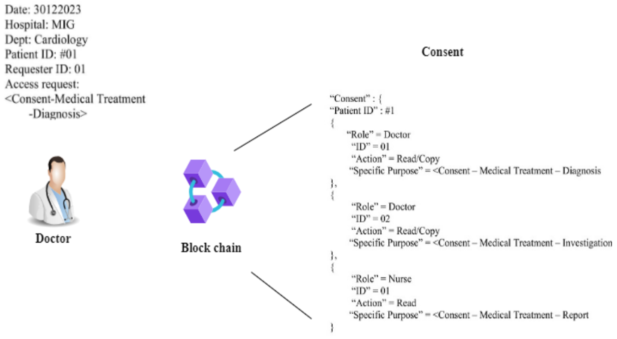
A nurse wishes to view a patient's data, in Fig. 2 and she submits an access request along with the data attributes and query terms. After the system has finished processing the data, it will check the patient's approval for each item in the list. The individual making the request can access and perhaps modify the data if it is in line with the patient's permission. So long as it has nothing to do with schooling or mental illness, she is free to access data for whatever reason.

Sample Request is shown below:

$$< Role, Id, Acess\ purpose, Action, >$$

Blockchain Protocol

Blockchain technology allows all members of a network to view and verify each other's transactions by recording them in a distributed ledger of blocks. According to Fig. 3, the hash value of one block is saved in the following block, which links them together (Viriyasitavat and Hoonsopon, 2019). This design feature renders the blockchain unchangeable; to change data in a block, one must first replace all other nodes' blockchains with their own forged one, then recalculate the block's hash using the changed data, and so on, until the last block.



Date: 30122023
Hospital: MIG
Dept: Cardiology
Patient ID: #01
Requester ID: 01
Access request:
<Consent-Medical Treatment
-Diagnosis>

```
"Consent" : {
"Patient ID" : #1
{
    "Role" = Doctor
     "ID" = 01
     "Action" = Read/Copy
    "Specific Purpose" = <Consent – Medical Treatment – Diagnosis
},
{
     "Role" = Doctor
     "ID" = 02
     "Action" = Read/Copy
    "Specific Purpose" = <Consent – Medical Treatment – Investigation
},
{
     "Role" = Nurse
     "ID" = 01
     "Action" = Read
    "Specific Purpose" = <Consent – Medical Treatment – Report
}
```

Fig. 2: Validation process of requester's access

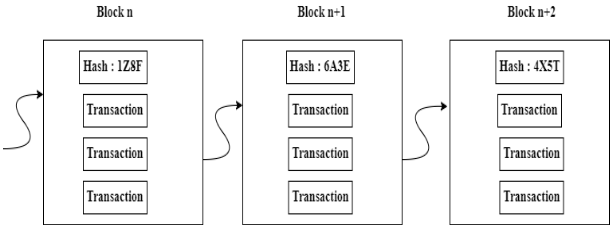


Fig. 3: Blockchain framework

This SCBCS method employs HL, a consortium blockchain where all members are located on the consortium's network, as our platform for the Blockchain. The HLF ledger is comprised of a blockchain and a global state database. There is a separate set that stores the program's final state variables (also called chain codes) and an immutable set of transactions (also called master transactions). Members of HLF can take advantage of the Membership Service Provider's (MSP) full suite of cryptographic capabilities, including user authentication through local Certificate Authorities (CAs), issuance and validation of Enrollment Certificates (ECerts) and their associated identifier, eID. User roles such as customer, endorser, and orderer are also provided by HLF. Upon validation, each endorser uses the chain code to officially support a tentative transaction, also known as a proposal. A block containing endorsed proposals is distributed among peers by an orderer for addition to the Blockchain.

As illustrated in Fig. 3, the identical system is modified to present the proposed model SCBCS. Patient's medical records are stored in the form of blocks and the information is protected using hash value for each block in Fig. 3. Participating hospitals, each with their own electronic health record system, can share patient records through a dedicated channel. In order to access their assigned roles in the system, members are required to have an ECert issued by the membership service provider. This ECert serves as the member's ID. The participating hospitals can be consulted in such a case. All hospital proxies work together to re-encrypt patient data and connect with other hospitals.

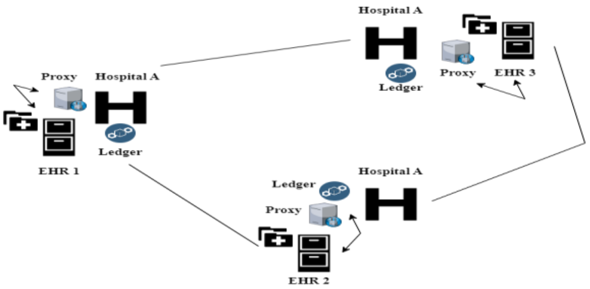


Fig. 4: Procedure of chain code among hospitals for exchange of Patient data

Procedure of Chain-Code

Network participants may agree on business logic and have it executed by a program called a chain code; this program functions similarly to an Ethereum smart contract. When users do transactions with it, they gain access to a blockchain. A chain code was developed to manage patient consent. Detailed below are the steps that make up the chain code. The procedure of the chain code is illustrated in Fig. 4. It shows that each medical organization maintains a proxy server, medical records, and distributed ledger and all are connected to share the information securely and effectively.

Consent Management

As illustrated below, this function coordinates patient consent by letting them access previous data, examine the consent, and update it in a blockchain. The purpose-tree is used to verify the format and authenticity of the proposal's intended purpose first. Next, it uses the patient's eID to search the blockchain for approval policies and transactions pertaining to the patient's medical records. Patients can revise their consents at any time by attaching new ones to the appropriate transactions in their medical records.

```
Input: Patient Proposal
Output: Message
Func_Consent(Patient Proposal):
if Patient Proposal == correct format then
    Query the blockchain for patient record
    transactions by ID and save the results in the
    array.
if the patient wants to upload a new consent of selected
    transaction then
    Append the new consent to the selected transaction
   Return message
else if the patient wants to update a consent in the selected
        transaction
        Remove the Old Consent
        Add the new consent to the selected transaction
 Return Message
```

Consent Check

This function compares the requestor's access request against the patient's consent that is stored in the blockchain. It verifies the requestor's position in the company and the proposal's format correctness after extracting the proposal.

After that, it uses the proposal's search terms to look for blockchain transactions. When the query is successful, the chain code checks the proposal's entities of access request against the characteristics of the patient's consent in the transactions. Lastly, no transactions will be issued by the chain-code until the patient's consents match the access request. Blockchain transactions include the URLs of records in EHR systems; these URLs are utilized to find the location of patient medical data, as previously stated. The consent check function is illustrated below:

```
Input: Access Request
Output: Record Data
Func_Consent_Check (Access Request):
        Query in the blockchain for Doctor role
        Compare the attributes and roles, retrieve the
        record.
        Return Patient Record Data
```

Implementation

Prototype System

A local network prototype using four Linux PCs to give a user interface for patients and doctors to request from the blockchain system is developed. After creating four endorser peers on PCs, chain codes were executed in Docker (https://www.docker.com/) to deploy the HLF platform. Additionally, HLF MSPs were installed on two PCs independently.

Prototype Analysis

The prototype system of the proposed method SCBCS is tested with three goals in mind:

1) Maintaining accurate patient records including those pertaining to consent creation, withdrawal, and updates
2) Validating the chain-code's intended purpose and access purpose against the purpose-tree
3) Determining if the chain code successfully validated a doctor's access request in light of the patient's consent to access the data

Because it was purposefully given the incorrect query results, which allowed it to identify a peer with the incorrect Blockchain. When constructing a block, the HLF consensus mechanism can verify it by comparing the outcomes from all peers who have endorsed it. Access request validation processing times were proportional to the length and complexity of each transaction's purpose tree and consent list. Meanwhile, the consortium's privacy regulations and legal constraints determine how quickly the proposal can be validated.

Results and Discussion

The proposed system "Smart Consent Blockchain-based System" (SCBCS) is compared with the existing system "MedRec”, proposed by Azaria *et al*. (2016), and the general consent management system without blockchain, namely CMS, which is in use, in some organizations across the world, in order to evaluate the performance. The efficacy of the proposed method SCBCS is showcased in terms of performance metrics like latency, cost analysis, and scalability.

Latency

The time it takes to collect individual data might be significantly reduced if people are more ready to contribute their data. Data providers' latency could differ. The below graph depicted in Fig. 5 exhibits the latency comparison of the proposed method SCBCS, MedRec, and existing CMS with respect to three data requestors and a data provider. The proposed method SCBCS exhibits an average latency of 268.25 ms, whereas MedRec shows 380 ms and CMS shows 445 ms. Table 1 shows the statistics of latency comparison in ms for the three methods. It is observed that SCBCS outperforms MedRec and CMS in terms of latency.

Cost Analysis

Gas is the cost of Blockchain transactions. Using the gas limit and gas pricing, the user's cost per unit of computation is defined. Gas is used for every ethereum contract deployment and transaction. Gas has economic worth and is paid in ether. The blockchain receives compiled code when you deploy a contract. Larger contract codes need more gas units when deployed. Gas, a measure of the computing effort necessary to execute an action, is used by every operation in the smart contract in the Ethereum ecosystem. Because different activities call for different amounts of processing power, gas consumption can vary. The smart contract's gas usage depending on the relevant actions, is compared and the identity of the person carrying them out (the data requester or the data provider). The overall cost of contract deployment is determined along with the cost of contacts between data providers and data requesters to help better grasp the costs involved. The overall expense of data sharing can be determined by adding together the costs of contract deployment, consent submission, and data querying for the data requesters. The graph in Fig. 6 displays the gas consumption amounts for various scenarios viz. proposed method SCBCS, MedRec method, and existing method CMS The majority of data requesters use more power than data suppliers, according to the graph. Their extensive use of data providers' smart contracts provides an explanation for this. More data sources may be approached to request access to their data if the stated objective is more general.

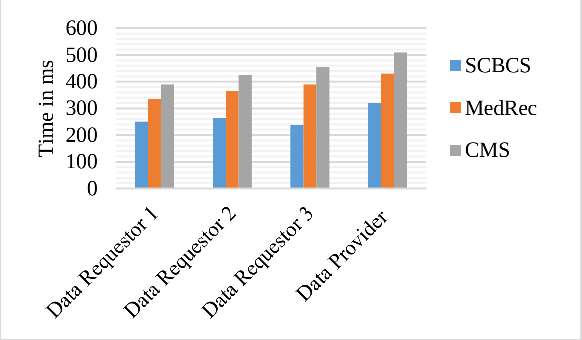


Fig. 5: Latency comparison of proposed SCBCS, MedRec, CMS

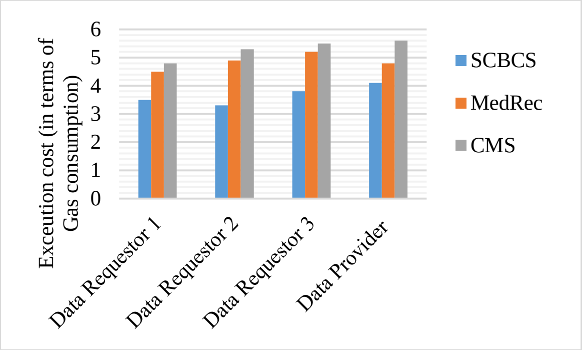


Fig. 6: Cost Analysis for proposed SCBCS, MedRec, CMS

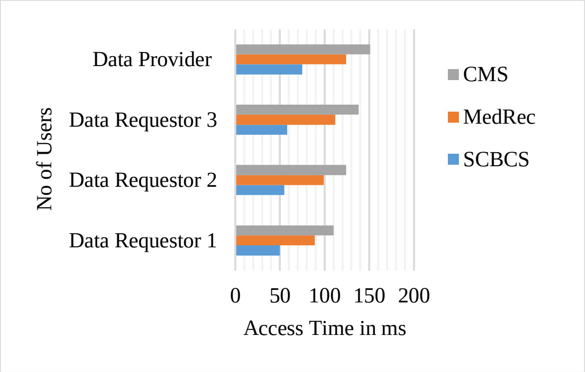


Fig. 7: Acces Time vs No of Users for proposed SCBCS, MedRec, CMS

Table 1: Latency statistics for SCBCS, MEdRec, and CMS

Latency in ms	SCBCS	MedRec	CMS
Data requestor 1	250	335	390
Data requestor 2	264	365	425
Data requestor 3	239	390	455
Data provider	320	430	510

Table 2: Cost analysis for SCBCS, MEdRec, and CMS

Gas Consumption	SCBCS	MedRec	CMS
Data requestor 1	3.5	4.5	4.8
Data requestor 2	3.3	4.9	5.3
Data requestor 3	3.8	5.2	5.5
Data provider	4.1	4.8	5.6

Table 3: Access time comparison for SCBCS, MEdRec, and CMS

Access time in ms	SCBCS	MedRec	CMS
Data requestor 1	50	89	110
Data requestor 2	55	99	124
Data requestor 3	58	112	138
Data provider	75	124	151

In the above graph, cost analysis is presented for three data req that depicts the Access Time uestors and one data provider. It is observed that the proposed SCBCS consumes gas at an average cost of 3.675, MedRec consumption is 4.85 and CMS is 5.3. This clearly shows the proposed method performs well in case of Cost incurrence when compared with the other two methods. Table 2 shows the statistics of the three methods in terms of cost analysis.

Scalability

Problems with scalability arise when the number of users on a blockchain platform grows. In contrast to the present approaches, which require organizations to physically submit consent forms, the proposed blockchain-based consent model SCBCS, offers greater flexibility. Smart contracts also make it such that a reliable third party isn't needed to handle the data processing at all.

This results in a decrease in the cost of data sharing between individuals or organizations. Using this technique, massive amounts of data can be quickly and efficiently processed within a constrained time frame. Because of unjust data-sharing procedures, a lot of data is currently being wasted. We anticipate a rise in personal data-sharing compliance with our methodology.

The graph in Fig. 7 depicts the access time comparison of the proposed method SCBCS with the other two methods MedRec and CNS.

It is observed that the proposed SCBCS exhibits 59.5 ms access time on average for all three data requesters and one data provider. MedRec shows an access time of 106 ms and the CNS shows an access time of 130.75 ms in the same case. This shows the proposed method performs well in the case of access time when compared with the other two methods. Table 3 shows the statistics of the three methods in terms of access time.

Conclusion

To ensure the confidentiality of medical records, patients must give their informed consent before any information can be shared. When given too liberally, patients run the danger of having their privacy compromised and when given too strictly, it creates problems when dealing with the data. As a result, patients would like to be able to track the usage of their consent-based data. They are hesitant to give data for research purposes and are generally inactive when it comes to data sharing unless proper measures are taken.

In this study, a novel electronic consent method that allows patients to more thoroughly govern their assent when it comes to data handling is presented. The RBAC concept of a relational database, namely its purpose-based access control method, was utilized in developing this method SCBCS. Patients would have a hard time understanding and consenting to the use of their data if our system combined the hierarchical structure of user roles with the hierarchical structure of user purposes. The idea behind the proposed system is patient-centric, in contrast to RBAC, which is role-based and focused on the institution. The proposed system supports the consent management system and access to patient health records based on a patient-centric approach. The patient will provide consent access to the specified health professional based on his role and very specific to the purpose mentioned.

Being a completely decentralized blockchain approach, the proposed solution differs from other purpose-based centralized platforms. Another blockchain-based option for dynamic consent in biobanking is the Dwarna project (Mamo *et al*., 2020). However, for their very basic study, they employ Boolean-based consent to grant requestors access to data.

Organizations that want to exchange data with one another will need to settle on a shared privacy policy, which could undermine the distinctive aspects of each member's policy. Complexity and reduced data usefulness result from the purpose tree's attempt to cover all participants' useful purposes with many branches at each node. The aim of this method is to make the model's principles straightforward and universally acceptable in order to address these inconsistencies.

The purpose-tree can be changed with the approval of participating organizations when privacy rules change or new organizations join. All organizations would need new patient consent because the new purpose tree would make it difficult to understand their current ones. A patient's contract can establish advanced protocols for such instances. Data issues including patients, have the "right of erasure" under the European General Data Protection Regulation (GDPR) (Intersoft Consulting, 2020) to delete their personally identifiable information. All blockchain-based systems struggle with this request because it violates the blockchain's immutability. Our method uses EHRs to store patient data off-chain to address this challenging problem.

Also, to further pseudonymize the data owner, it makes sure that each on-chain transaction has a unique hash number of the patient's eID with a random number, also known as a salt (Gauravaram, 2012), even if this slows down data searching performance. The off-chain database stores the link that links the randomized patient eID to off-chain records. If a patient requests the erasure of their data, the system will remove both the link and the off-chain record. The patient's information could be gleaned from the URL provided in the transaction, which is the location of the EHR data site; however, this is extremely challenging to accomplish because of the shared nature of the URL. While the patient record and consent are kept off-chain, the hash is kept on-chain to ensure data integrity. Like other blockchain systems, the proposed method is very transparent and easy to track and it has great availability and reliability. In order to guarantee the correct sharing of patient data, transparency, and traceability are particularly vital when dealing with patient permission.

The proposed method SCBCS is designed to facilitate patient data sharing across hospitals and also facilitate data donation for bio-banking research.

Acknowledgment

The authors acknowledge the support and cooperation rendered by all the members directly and indirectly. All the authors were involved actively in the proposed work. Author 1 was active in all the sections. Author 2 was specific in concluding the survey part. Author 3 analyzed the results based on the findings.

Funding Information

The authors have not received any financial support or funding to report.

Author’s Contributions

K. R. Rohini: Content written, designed, collection of data, novelty.

P. S. Rajakumar: Refinement of content, checked the novelty and flow of work.

S. Geetha: Checked for final approval of the article in all aspects.

Ethics

This article is written adhering to all the ethical standards that are necessary.

References

Aldred, N., Baal, L., Broda, G., Trumble, S., & Mahmoud, Q. H. (2019). Design and implementation of a blockchain-based consent management system. *arXiv preprint arXiv: 1912.09882*. https://doi.org/10.1109/SMC42975.2020.9283203

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *In Proceedings of the 13th EuroSys Conference*, (pp. 1-15). https://doi.org/10.1145/3190508.3190538

Asghar, M. R., & Russello, G. (2012). Flexible and dynamic consent-capturing. In *Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2011, Lucerne, Switzerland, June 9, 2011, Revised Selected Papers* (pp. 119-131). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27585-2_10

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. *In 2016 2nd International Conference on Open and Big Data* (*OBD*), (pp. 25-30). IEEE.

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials*, *18*(1), 1-5. https://doi.org/10.1186/s13063-017-2035-z

Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., ... & Suen, C. H. (2018, April). Double-blind consent-driven data sharing on blockchain. *In 2018 IEEE International Conference on Cloud Engineering* (*IC2E*), (pp. 385-391). IEEE. https://doi.org/10.1109/IC2E.2018.00073

Byun, J. W., & Li, N. (2008). Purpose based access control for privacy protection in relational database systems. *The VLDB Journal*, *17*, 603-619. https://doi.org/10.1007/s00778-006-0023-0

Byun, J. W., Bertino, E., & Li, N. (2005, June). Purpose based access control of complex data for privacy protection. *In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies*, (pp. 102-110). https://doi.org/10.1145/1063979.1063998

Cha, S. C., Chen, J. F., Su, C., & Yeh, K. H. (2018). A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access*, *6*, 24639-24649. https://doi.org/10.1109/ACCESS.2018.2799942

Cha, S. C., Tsai, T. Y., Peng, W. C., Huang, T. C., & Hsu, T. Y. (2017, October). Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. *In 2017 IEEE 6th Global Conference on Consumer Electronics* (*GCCE*), (pp. 1-3). IEEE. https://doi.org/10.1109/GCCE.2017.8229327

Coiera, E., & Clarke, R. (2004). E-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association*, *11*(2), 129-140. https://doi.org/10.1197/jamia.M1480

Copigneaux, B. (2014, March). Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the Internet of Things. *In 2014 IEEE World Forum on Internet of Things* (*WF-IoT*), (pp. 411-416). IEEE. https://doi.org/10.1109/WF-IoT.2014.6803201

CIOMS. (2016). International ethical guidelines for health-related research involving humans. *(No Title)*. *Council for International Organizations of Medical Sciences*. https://cir.nii.ac.jp/crid/1360016870543307904

Gauravaram, P. (2012). Security analysis of salt||password hashes. *Proceedings of 2012 International Conference on Advanced Computer Science Applications and Technologies* (ACSAT) 26-28; Kuala Lumpur, Malaysia. p. 25-30. https://doi.org/10.1109/ACSAT.2012.49

Hyperledger. (2020). What is Hyperledger Fabric [Internet]. Dublin, Ireland. https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html.

ICH E6(R1). (2016). Guideline for good clinical practice E6(R2) [Internet]. International Council for Harmonisation. November 9, 2016. https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf

Intersoft Consulting. (2020). General Data Protection Regulation. (2020) Art. 17 GDPR: Right to erasure (‘right to be forgotten’) [Internet]. https://gdpr.eu/article-17-right-tobe-forgotten/

Kabir, M. E., Wang, H., & Bertino, E. (2011). A conditional purpose-based access control model with dynamic roles. *Expert Systems with Applications*, *38*(3), 1482-1489. https://doi.org/10.1016/j.eswa.2010.07.057

Kish, L. J., & Topol, E. J. (2015). Unpatients-why patients should own their medical data. *Nature Biotechnology*, *33*(9), 921-924. https://doi.org/10.1038/nbt.3340

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *In 2016 IEEE Symposium on Security and Privacy* (*SP*), (pp. 839-858). IEEE. https://doi.org/10.1109/SP.2016.55

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017, May). Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. *In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (*CCGRID*), (pp. 468-477). IEEE. https://doi.org/10.1109/CCGRID.2017.8

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, *19*(5), 653-659. https://doi.org/10.6633/IJNS.201709.19(5).01

Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J. P. (2020). Dwarna: A blockchain solution for dynamic consent in biobanking. *European Journal of Human Genetics*, *28*(5), 609-626. https://doi.org/10.1038/s41431-019-0560-9

Nakamoto, S. (2016). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper.

Neisse, R., Baldini, G., Steri, G., & Mahieu, V. (2016, May). Informed consent in Internet of Things: The case study of cooperative intelligent transport systems. *In 2016 23rd International Conference on Telecommunications* (*ICT*), (pp. 1-5). IEEE. https://doi.org/10.1109/ICT.2016.7500480

Neisse, R., Steri, G., & Nai-Fovino, I. (2017, August). A blockchain-based approach for data accountability and provenance tracking. *In Proceedings of the 12th International Conference on Availability, Reliability and Security*, (pp. 1-10). https://doi.org/10.1145/3098954.3098958

Ramachandran, A. & Kantarcioglu, M. (2017). Using blockchain and smart contracts for secure data provenance management. arXiv:1709.10000. http://arxiv.org/abs/1709.10000

Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., & Filippidis, A. P. (2019). A blockchain-based platform for consent management of personal data processing in the IoT ecosystem. *Security and Communication Networks*, *2019*, 1-15. https://doi.org/10.1155/2019/1431578

Riggs, E. R., Azzariti, D. R., Niehaus, A., Goehringer, S. R., Ramos, E. M., Rodriguez, L. L., ... & Clinical Genome Resource Education Working Group. (2019). Development of a consent resource for genomic data sharing in the clinical setting. *Genetics in Medicine*, *21*(1), 81-88. https://doi.org/10.1038/s41436-018-0017-5

Stanley, A. (2021). Big pharma seeks DLT solution for drug costs. https://www.coindesk.com/blockchain-day-big-pharma-seeks-dltsolution-drug-costs

Tith, D., Lee, J. S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Informatics Research*, *26*(4), 265. https://doi.org/10.4258/hir.2020.26.4.265

Vest, J. R., & Gamm, L. D. (2010). Health information exchange: Persistent challenges and new strategies. *Journal of the American Medical Informatics Association: JAMIA*, *17*(3), 288. https://doi.org/10.1136/jamia.2010.003673

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32-39. https://doi.org/10.1016/j.jii.2018.07.004

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. *In 2016 IEEE International Conference on Consumer Electronics* (*ICCE*), (pp. 467-468). IEEE. https://doi.org/10.1109/ICCE.2016.7430693

World Medical Association. (2018). WMA Declaration of Helsinki – ethical principles for medical research involving human subjects [Internet]. https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

World Medical Association. (2013). World Medical Association Declaration of Helsinki Ethical Principles for Medical Research Involving Human Subjects https://doi.org/10.1001/jama.2013.281053

Wuyts, K., Scandariato, R., Verhenneman, G., & Joosen, W. (2011). Integrating patient consent in e-health access control. *International Journal of Secure Software Engineering* (*IJSSE*), *2*(2), 1-24. https://doi.org/10.4018/jsse.2011040101

Zhang, R., George, A., Kim, J., Johnson, V., & Ramesh, B. (2019). Benefits of blockchain initiatives for value-based care: Proposed framework. *Journal of Medical Internet Research*, *21*(9), e13595. https://doi.org/10.2196/13595

Zhuang, Y., Sheets, L. R., Shae, Z., Chen, Y. W., Tsai, J. J., & Shyu, C. R. (2019). Applying blockchain technology to enhance clinical trial recruitment. *In AMIA Annual Symposium Proceedings* (Vol. 2019, p. 1276). American Medical Informatics Association. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153067/

Zhuang, Y., Sheets, L., Shae, Z., Tsai, J. J., & Shyu, C. R. (2018). Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. *In AMIA Annual Symposium Proceedings* (Vol. *2018*, p. 1167). American Medical Informatics Association.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE Security and Privacy Workshops*, (pp. 180-184). IEEE. https://doi.org/10.1109/SPW.2015.27