PLOS ONE

RESEARCH ARTICLE

PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records

Bello Musa Yakubu[1], **Syeda Mahera Ali**[2], **Majid Iqbal Khan**[2], **Pattarasinee Bhattarakosol**[1]*

1 Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand, **2** Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan

* pattarasinee.b@chula.ac.th

Citation: Yakubu BM, Ali SM, Khan MI, Bhattarakosol P (2024) PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records. PLoS ONE 19(9): e0310407. https://doi.org/10.1371/journal.pone.0310407

Editor: Shadab Alam, Jazan University, SAUDI ARABIA

Received: January 22, 2024

Accepted: August 31, 2024

Published: September 18, 2024

Data Availability Statement: all data supporting our findings are included within the manuscript, and the associated code that underpins our findings is available in a public GitHub repository for ease of access and verification at the following URL: https://github.com/sysbel07/PatCen.git.

Funding: This research is supported by Ratchadapisek Somphot Fund for Postdoctoral Fellowship, Chulalongkorn University, Bangkok, Thailand. Authors are thankful for the support. the funders had no role in the study design, data

Abstract

The recent global outbreaks of infectious diseases such as COVID-19, yellow fever, and Ebola have highlighted the critical need for robust health data management systems that can rapidly adapt to and mitigate public health emergencies. In contrast to traditional systems, this study introduces an innovative blockchain-based Electronic Health Record (EHR) access control mechanism that effectively safeguards patient data integrity and privacy. The proposed approach uniquely integrates granular data access control mechanism within a blockchain framework, ensuring that patient data is only accessible to explicitly authorized users and thereby enhancing patient consent and privacy. This system addresses key challenges in healthcare data management, including preventing unauthorized access and overcoming the inefficiencies inherent in traditional access mechanisms. Since the latency is a sensitive factor in healthcare data management, the simulations of the proposed model reveal substantial improvements over existing benchmarks in terms of reduced computing overhead, increased throughput, minimized latency, and strengthened overall security. By demonstrating these advantages, the study contributes significantly to the evolution of health data management, offering a scalable, secure solution that prioritizes patient autonomy and privacy in an increasingly digital healthcare landscape.

Introduction

In the past, infectious diseases such as yellow fever, Ebola, smallpox, monkeypox, and influenza were among the most feared epidemics. Nowadays, new infections like COVID-19 continue to emerge, while many old epidemics persist, posing global challenges. The rapid spread of infections, exemplified by the COVID-19 pandemic, demonstrates how a new disease can traverse continents within days or weeks [1, 2]. To curb the spread of such diseases, many countries have resorted to strategies such as lockdowns, albeit at the cost of disrupting economic growth [3, 4]. Infectious diseases disproportionately affect vulnerable populations, including those with existing health conditions, children, and individuals over 60 [4–6]. Each

collection, analysis, decision to publish, or manuscript preparation.

Competing interests: The authors have declared that no competing interests exist.

infectious disease presents a variety of symptoms, ranging from cough, fever, and fatigue to more severe complications like lung damage, and sensory impairments [4].

One of the most concerning aspects of infectious diseases is the potential for asymptomatic transmission, wherein carriers may spread the disease without exhibiting symptoms [4, 7]. Therefore, infected individuals are required to self-isolate for at least 14 days, the typical incubation period for many diseases, during which they may unknowingly transmit the virus to others [8]. Many countries and organizations have subsequently recommended widespread testing to prevent the spread of diseases. However, publication delays caused by intermediaries and inconsistencies in action plans may thwart effective response strategies.

Recently, researchers have proposed various techniques to address these challenges, such as storing results data in a blockchain public ledger [9, 10]. This approach allows government agencies and organizations to access patient data for infection monitoring, subject to patient consent. This purpose has utilized two types of blockchains: permissioned [11–15] and permissionless [16–20]. Permissioned blockchains are private networks with known users, managed by centralized organizations, while permissionless blockchains operate on peer-to-peer networks and are open to the public [11, 16].

Despite their potential, permissioned blockchains face challenges such as data confidentiality and scalability issues, whereas permissionless blockchains offer tamper-resistant storage and transfer of information. Techniques such as [12, 21–24] have proposed various methods to enhance health record access control, aiming to address privacy risks associated with unauthorized access to patient data. However, they fall short in several areas: they lack mechanisms for privilege designation and authorization, infringe on patient rights by omitting consent requirements, and inadvertently expose sensitive patient data to unauthorized entities [4–6]. These shortcomings not only compromise data privacy and security but also hinder the effective deployment of health interventions during crises [21, 23].

This study presents a blockchain-based approach utilizing self-triggering smart contracts to establish trust and prevent fraud in healthcare systems. By leveraging digital medical credentials and permissioned blockchain technologies, the model facilitates reliable and timely reporting of infectious diseases. Patients can grant access to authorized organizations, verified through unique identification, to support response strategies against disease spread. This approach ensures data integrity and patient privacy while enabling efficient information sharing among stakeholders.

Furthermore, our study illuminates the critical role of blockchain in enhancing EHR access control, offering a detailed examination of its potential to resolve prevalent issues related to data privacy, scalability, and unauthorized access. This work significantly contributes to the discourse on digital health record management and patient empowerment in the era of blockchain technology by presenting a comprehensive security analysis and leveraging game theory to evaluate the proposed model's robustness.

This article makes several pivotal contributions to the field of healthcare data management and security, leveraging the power of blockchain technology. An enhanced presentation of these contributions is provided below:

- Innovative Access Control Framework: At the heart of this research is the creation and deployment of an innovative access control framework tailored for the healthcare sector. Building upon the robust functionalities of blockchain technology, this framework establishes a new benchmark for secure and efficient data management in healthcare systems.
- Empowering Patients with Data Control: Our study significantly advances patient empowerment by providing them with clear control over their medical records. By enabling informed decision-making, our approach not only fortifies data privacy but also adapts to diverse data

access requirements. The novel paradigm it introduces enhances data privacy safeguards, fine-tunes access privileges, and adeptly addresses scalability challenges, all while upholding the sanctity of patient privacy.

- Synergy Between Patient Empowerment and E-Health Services: This study further explores and elucidates the symbiotic relationship between patient empowerment and the efficacy of electronic health (e-health) services. It demonstrates how blockchain technology's inherent strengths can amplify the benefits of e-health services, thereby fostering a more secure, efficient, and user-centric healthcare ecosystem.
- Rigorous Security Evaluation: Our research conducts an extensive security evaluation of the proposed blockchain-based solution using Decisional Bilinear Diffie-Hellman (DBDH) game theory. Additionally, we conduct a comprehensive security analysis using the Real-Or-Random (ROR) game theory approach to meticulously assess the security features of the session key mechanism. These studies validate the proposed solution's robustness against various security threats, ensuring a secure and trustworthy framework for healthcare data management.

Through these contributions, our study not only addresses critical gaps in current healthcare data management practices, but also lays the groundwork for future advancements in the secure and effective use of blockchain technology in healthcare and beyond.

The rest of this paper is structured to build upon the foundation laid in this introduction, starting with a detailed literature review that contextualizes our research within the broader field. Subsequent sections delve into the system model, elucidate the proposed PatCen model, offer a thorough security analysis, and present empirical findings from our evaluations, leading to a concluding discussion that highlights key insights and future directions for research in this vital area.

Literature review

In recent years, several academics have dedicated their efforts to examining the various obstacles and possibilities associated with the integration of blockchain technology into e-health systems [25–27]. This line of inquiry has also included the identification of prospective avenues for further investigation, with a particular focus on the management of patient data access [28]. The concept of EMRs and their prototype, referred to as "MedRec", was first proposed by Azaria et al. [29] and Hongwei et al. [30] using blockchain-based management framework. Similarly, a blockchain-based e-healthcare system was introduced by [23], which interacts with wireless body area networks using Hyperledger Fabric, achieving good performance in terms of hardware utilization, security, and system stability. However, these frameworks [29, 30] are associated with scalability constraints and can only accommodate a maximum of 51 nodes. To address this issue, a Hyperledger-based e-health technique was introduced in [15, 23] to increase the reliability and stability of e-health services, such as automating healthcare record sharing. However, the scalability issue is inevitable, thus, it is worth noting that these frameworks [15, 23, 29, 30] see medical facilities as the focal point for researching security and productivity challenges, while patients' privileges are ignored [31].

The significance of allowing patients to grant access to their own medical data was stressed and discussed in [32]. As a result, several works, like [33–36], proposed a patient-centric healthcare data management scheme for privacy preservation. While [37, 38], talked about patient-driven healthcare interoperability and showed how smart contracts can protect the privacy of electronic health records, the authors of [39] used smart contracts to set up an e-health framework that lets a doctor access patient data through system notifications for real-time

monitoring. To make hospitals' records more accessible, [40] proposed a patient-centric model based on smart contracts; however, no robust trial protocol is provided. Correspondingly, [41, 42] proposed a blockchain-based medical data collection scheme and a mixed blockchain-edge architecture, respectively. Similarly, the authors in [43] proposed a blockchain-based network for smart healthcare systems called "S2HS," in which doctors or practitioners can access data only if patients want to share their medical data. Moreover, [44, 45] used blockchain technologies for healthcare management, allowing the emergency department to view patient medical records in an emergency without the patient's permission. The various works described above are patient-centric, meaning that anyone who accesses medical data must obtain patient consent. Patients' rights are undoubtedly well-protected, but this approach also constrains the practicality of e-health services, raising privacy and security concerns like high latency, storage costs, and a single point of failure [46, 47].

Numerous access control approaches for health records have been suggested in the literature [12, 21, 23], with the aim of enhancing security. However, it has been observed that in real-world scenarios, unqualified or unauthorized third parties may gain access to the transaction content of approved third parties, therefore compromising the privacy of patient data [22, 48]. The problem at hand is exacerbated by the use of security techniques that are deemed ineffective, such as public session key security and the existence of transparency concerns within blockchain technology [10, 22]. In current EHR systems, it is common for third parties to use public keys or Ethereum addresses. This practice, however, poses a risk as it might potentially reveal the real identities of these third parties and thereby expose patients' confidential information to unauthorized individuals. The aforementioned scenario has the potential to give rise to dangers connected to anonymity, hence rendering patients' sensitive information susceptible to illegal access [10, 22, 48].

To revolutionize smart healthcare record systems by ensuring patients' rights are well secured and providing real-time services, with improved privacy and security, authors in [49] have proposed a technique termed "Bloccess", a fine-grained access control framework based on the consortium blockchain. By leveraging blockchain technology, they formulate a set of protocols to enforce a tamper-proof access control mechanism in untrustworthy distributed environments. Similarly, the authors of [50, 51] propose a patient-driven blockchain-based architecture that provides decentralized EHR and smart-contract-based service automation without compromising system security and privacy. In a similar vein, the authors in [47] put out a proposition that enables patients to bestow and withdraw access privileges, while also safeguarding the privacy of healthcare institutions and practitioners. Cloud storage is used to store sensor data, while blockchain is used to maintain access control and session records. The solution employed a data-driven authentication and secure communication protocol, utilizing smart contracts to regulate interactions between the cloud, patients, and healthcare professionals. However, these approaches are susceptible to high latency, high throughput, high computational overhead, and availability issues. Similarly, the approaches may lead to external or internal unauthorized access to sensitive EHR attributes for malicious purposes, patient privacy issues and privilege exploitation [27, 52].

The authors of [53] present a patient-driven approach, known as the triple subject purpose-based access control (TS-PBAC) model, for secure and privacy-preserving IoMT access control, to address issues related to system performance, privacy, and unauthorized access to sensitive EHR attributes. They create hierarchical purpose trees (HPT) and policies to ensure that external users are legal. To enhance the privacy of sensitive attributes, they also introduce LDP-based policies and role-based access control schemes in edge computing. They introduce mutual evaluation metrics using blockchain-enabled records to assess data quality at the patient and medical service levels within an open, anonymous network. Likewise, the authors

of [54] present another patient-driven approach that considers the InterPlanetary Health Layer and related Internet of Medical Things (IoMT) implementations. The approach's primary objective is to manage sensitive data while protecting privacy and ensuring data availability. Specifically, without relying on a third party, users can construct their own private network, collaboratively authorize data operations, and administer their privacy settings. However, patient privacy remains susceptible to data intrusions in these approaches, despite the use of blockchain-based security for electronic health records [55]. Similarly, diverse privileges and scalability present complications for access control systems [56].

To address the issues related to security and privacy concerns, the authors in [57] propose a patient-centric blockchain-based self-sovereign identity (SSI) paradigm for a decentralized self-management of data access control (DSMAC) system. This system enables patients to maintain control over their personal information and grant themselves access to their medical records. In emergency situations, DSMAC employs smart contracts for role-based access control policies, as well as decentralized identifiers and verifiable credentials for advanced access control techniques. Similarly, the authors of [58] introduced a patient-driven approach that scrutinizes the prerequisites for a generalized health passport system. They employ agent-oriented modeling (AOM) to create a blockchain-based self-sovereign identity (SSI) system that integrates with the personal health record (PHR), safeguarding end-users' privacy and empowering them to manage the data they utilize for credential verification. Even though these approaches have strengthened blockchain-based e-health services in many respects, they have not expressly considered patients' privileges [27]. Table 1 provides a summary of the most similar existing approaches.

Several other studies have provided significant perspectives on how blockchain can enhance security, privacy, and efficiency in several fields, which closely aligns with PatCen's goals. Sharma et al. (2023) [55] introduces a framework that leverages blockchain technology to safeguard privacy in healthcare systems powered by the IoT. The framework offers a decentralized method for organizing medical records. Gaur et al. (2023) [59] emphasizes the need for strong security measures to defend against adversarial attacks in cyber-physical systems, emphasizing the necessity of safeguards to guarantee the integrity of data. Zhang et al. (2023) [60] provide a system for privacy-preserving distant sensing picture identification that uses visual

Table 1. Literature review.

References	Objectives	1	2	3	Limitations
[15, 23, 29, 30]	The blockchain-based management system to handle EMRs	×	×	✓	Third party privileges are not considered, no classification of data.
[32, 33]	Patient's data access management mechanisms to address the issue of patients' privileges	×	✓	×	Patients' privileges are not considered, plus none-patient driven.
[49–51]	Patient's data access management mechanisms to address the issue of user privileges	×	✓	×	User privileges are considered except the patients' privileges, none-patient centric.
[53, 54]	Patient's data access management mechanisms to address the issue of data privacy	×	×	✓	Patient privileges are not considered, including diverse privileges and scalability complications.
[12, 21, 23, 57, 58]	Patient-centric healthcare data access management scheme for privacy preservation.	×	×	✓	Patient centric, Patients' privileges are not fully considered.
[34–36, 43],	Patient-centric healthcare data management scheme for privacy preservation.	×	✓	×	Patients' privileges are not considered, including none-patient driven.
[37, 38, 40, 41]	To protect the privacy of electronic health records.	×	×	✓	Third party privileges are not considered, and have no classification of data.
[42, 45]	To view patient medical records in an emergency without the patient's permission	✓	×	×	Patient centric, patients' privileges are not fully considered.

1: Patients have partial control over their records. **2**: Patients have no control over their records. **3**: Patients have full control over their records.

https://doi.org/10.1371/journal.pone.0310407.t001

cryptography. This highlights how important it is to protect patient privacy with private medical information. D. Charles (2023) [61] studied a cross-border payment system that demonstrates the versatility and growth potential of blockchain technology, essential for its potential expansion and seamless integration with other systems. A prevalent technological vulnerability found in these models is the intricate nature and demanding processing needs linked to blockchain and cryptography methods. This can result in longer response times and decreased efficiency, making it difficult to deploy these systems on a broad scale [62].

Problem statements and objectives of the study

The scholarly inquiry within the domain of blockchain-based e-health systems predominantly revolve around two central themes: data access management and privacy preservation. However, there exists an imperative need for the development of a comprehensive access control framework that places paramount importance on patient-centric principles and exhibits adaptability to diverse access scenarios, all while upholding the inherent rights and privileges of the involved patients. Presently, prevailing methodologies often overlook the crucial aspects of data classification, patients' rights and privileges, and inadequately address the intricate challenges posed by scalability.

Preliminaries

This section discusses the preliminaries of the overall system model, including the network model, adversary model, system requirements and data classification and its impact on access control in proposed system.

Network model

The utilization of a decentralized private Ethereum blockchain forms the backbone of our network architecture. Ethereum blockchain, renowned for its robustness, transparency, and smart contract functionalities, provides a secure and immutable platform for our data sharing ecosystem. As depicted in Fig 1, the network comprises four key stakeholders: users (third parties), patient, laboratories, administrator (admin), each possessing distinct Ethereum accounts

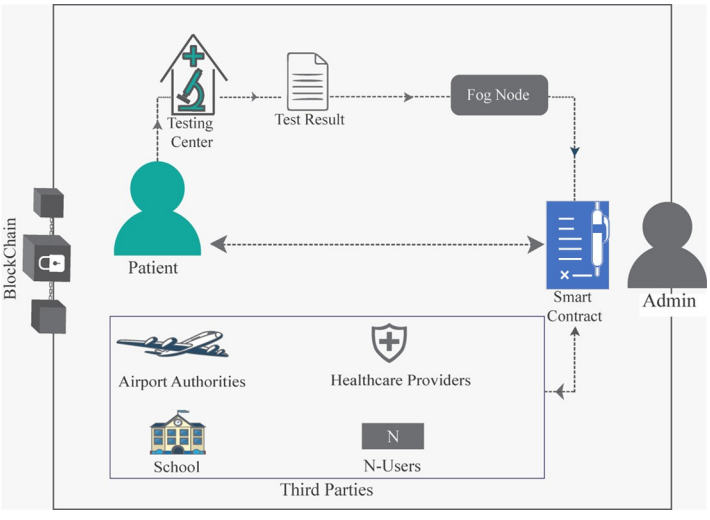

Fig 1. Network model.

https://doi.org/10.1371/journal.pone.0310407.g001

(EA). The admin plays a pivotal role in system governance by registering stakeholders and overseeing their participation.

The patient, acting as the data owner, initiates the data sharing process by providing samples and relevant information to laboratories. This information may be related to medical, educational, or travel-related data. Meanwhile, laboratories utilize sample processing devices to generate test results. These results as well as the associated relevant information are securely uploaded to the blockchain via fog nodes, ensuring accessibility while maintaining data integrity. Subsequently, access permissions are granted to other users as necessitated, further reinforcing the patient's control over their data. The data access granting process is facilitated through a mobile application, wherein the patient verifies and grants access permissions to requesting users via the smart contract.

Users, representing third-party entities, seek access to patient records within the system via smart contract based on predefined roles. Access permissions are granted for specified durations, with provisions for extension upon request. Notably, the patient retains ownership of their data and may grant access to authorized users when needed. This dynamic access control mechanism ensures data privacy and security while facilitating seamless information exchange.

By leveraging the Ethereum blockchain, our network guarantees transparency, immutability, and security, thereby establishing a robust foundation for patient-centric data sharing in healthcare and beyond.

Adversarial model

In this work, we assume that the adversary can conduct a sequence of malicious attacks on the system and may possess the following capabilities:

1. *Direct Data Attacks*: The adversary may attempt to directly attack the patient's data to gain unauthorized access or steal data stored in the public ledger. This includes techniques such as hacking into the system, exploiting software vulnerabilities, or launching phishing attacks to obtain sensitive information.
2. *Unauthorized Third-Party Attacks*: The adversary may be an unauthorized third party who tries to infiltrate the network to access data. This type of adversary could leverage social engineering, network eavesdropping, or brute force attacks to gain unauthorized access to the blockchain network.
3. *Insider Threats*: The adversary may be an authorized third-party user who seeks to access data beyond their intended scope (e.g., an educational user attempting to access travel-related health information). This insider threat scenario highlights the risk of privilege escalation and the need for strict access controls.
4. *Blockchain Integrity Assumption*: We assume that the blockchain itself is secure and cannot be compromised. This assumption is based on the inherent security properties of blockchain technology, such as cryptographic hashing, decentralized consensus mechanisms, and immutability.

System requirements

1. The system needs to preserve safe data sharing with legitimate third-party users based on their purpose.

2. The system fails when access permission is given to a legitimate user with a different purpose or when access is given to a non- legitimate user with or without the permission of the patient.

Data classification and its impact on access control in proposed system

In the proposed system, data classification is a fundamental component designed to protect sensitive healthcare information, specifically focusing on infectious disease test records. This classification system is tailored to the needs of the four key stakeholders involved: patients, laboratories, administrators, and third-party users (e.g., airport authorities, healthcare providers, and educational institutions). The classification of data directly influences how access is controlled, ensuring that each stakeholder can access the appropriate information necessary for their role while maintaining the security and privacy of patient records.

Types of data classified. The proposed system classifies infectious disease test records and related data into distinct categories, each with specific access permissions based on the stakeholder's role:

1. **Patient information:**
   - **Examples:** Patient identifiers, consent records, and historical test results.
   - **Classification impact:** This data is highly sensitive and primarily accessible to the patient and the laboratory that generates the test results. Patients have the authority to control who else can access this information, such as third-party users for specific purposes (e.g., travel clearance). The system ensures that patients can selectively share their information with authorized third parties while maintaining control over their data.
2. **Laboratory data:**
   - **Examples:** Test results, laboratory notes, and diagnostic reports.
   - **Classification impact:** Laboratory data is restricted to the laboratory that generates the test results and the patient. Laboratories are responsible for securely uploading this data to the blockchain, where it is then accessible to the patient. The laboratory data is also made available to third-party users only when the patient grants explicit permission. This classification ensures that test results remain confidential until the patient decides to share them.
3. **Third-party access data:**
   - **Examples:** Data requested by third parties such as airport authorities, healthcare providers, or educational institutions.
   - **Classification impact:** Third-party access data is governed by the permissions set by the patient. For instance, if a patient needs to provide proof of a negative test result for travel purposes, they can grant specific access to the relevant airport authority. The system enforces these permissions through smart contracts, ensuring that third-party users only access the data necessary for their specific use case and only within the scope defined by the patient.
4. **Administrative data:**
   - **Examples:** System logs, user access records, and permission settings.
   - **Classification impact:** Administrative data is primarily accessible to system administrators, who are responsible for managing the blockchain infrastructure, ensuring compliance

with regulatory standards, and monitoring the system for any unauthorized access. This data includes logs of all access requests and permissions granted, providing a transparent audit trail. Administrators do not have access to the actual test results or patient identifiers unless explicitly permitted by the patient for system maintenance or legal compliance purposes.

Impact on access control. The classification of data within the proposed system directly influences how access control mechanisms are implemented for each stakeholder:

- **Patient-centric control:** Patients are at the centre of the access control process, with the ability to manage who can access their infectious disease test records. The classification ensures that patients can selectively share their data with third parties based on the specific needs of each situation (e.g., traveling, healthcare, education) while retaining overall control over their personal health information.
- **Laboratory-patient confidentiality:** The direct communication channel between laboratories and patients ensures that test results are only shared when necessary. Laboratories upload the results to the blockchain, but the data remains confidential until the patient chooses to share it with a third party. This classification supports strict confidentiality and minimizes the risk of unauthorized access to sensitive health data.
- **Third-party access regulation:** Third-party users, such as airport authorities or healthcare providers, are only granted access to the data that the patient deems necessary. This is enforced through the smart contracts embedded in the blockchain, which ensure that access is both limited in scope and time-bound, preventing misuse or overreach.
- **Administrative oversight:** Administrators have access to system-level data, which allows them to manage the blockchain and enforce compliance without compromising patient privacy. The classification ensures that administrators can perform their duties without accessing sensitive health information unless specifically required for system integrity or legal compliance.

The data classification system in proposed system is tailored to the unique roles and responsibilities of the key stakeholders involved in managing infectious disease test records. By categorizing data based on its relevance and sensitivity to each stakeholder, PatCen ensures that access to healthcare information is strictly controlled, supporting patient privacy while enabling necessary interactions with third-party users. This classification-driven access control mechanism is central to the security and effectiveness of the proposed system, ensuring that sensitive data is handled in a secure, transparent, and patient-centred manner.

Proposed PatCen model

This section provides a detailed description of the proposed patient centric (PatCen) model's structure. The model consists of two distinct components: first, the granular data access control mechanism, followed by the second, the attribute-based data confidentiality scheme. These two components are distinctive and considerably contribute to the proposed PatCen model's security and efficient implementation. The subsequent subsections provide detailed explanations of the procedures involved. Table 2 provides descriptions of some important symbols used in the proposed model.

Table 2. Key terms and descriptions.

Symbol	Description	Symbol	Description
RID	Requester ID	TK	Encrypted text
$\boldsymbol{\theta}$	Validity period	ϑ	Other vital information associated with patient or third-party user
$\boldsymbol{RBK_i}$	User i public key	Đ	Data
$\boldsymbol{Gateway_{id}}$	Admin ID	M	Original message
$\boldsymbol{RType}$	Third-party user's request type	U_y	Users (general)
$\boldsymbol{List_i}$	A given list	U_{y1U}	Third-party user
$\boldsymbol{IndexList_i}$	A given Index list	U_{y2G}	Gateway (admin) user
$\boldsymbol{request_i}$	A given request	U_{y3P}	Patient user
$\mathcal{G}'$ and $\mathcal{G}''$	Multiplicative cyclic groups of prime order $\boldsymbol{p}$	$\mathcal{A}$	Adversary
$\boldsymbol{\hbar}$	The generator of $\mathcal{G}'$	$hf(.)$	Hash function
$\boldsymbol{\hbar}$	A bilinear map function	K_{pub}	Public key
$\boldsymbol{x,y} \in$	Elements of $\mathcal{G}'$	M_K	Master key
$\boldsymbol{s,t,w}$	Elements of $\mathbb{Z}_{\boldsymbol{p}}$	K_{prv}	Private key
$\boldsymbol{A_{atr} = \{a_1 \ldots \ldots, a_N\}}$	A set of attributes	$\delta, \delta', h_2, \varphi_1, \varphi_2, \sigma, \eta, \rho$	Random values
$\boldsymbol{U}$ and $\boldsymbol{AS}$	Attribute list of users and access structures, respectively	DBDH	Decisional Parallel Bilinear Diffie-Hellman Exponent

https://doi.org/10.1371/journal.pone.0310407.t002

Granular data access control mechanism

This section presents a thorough clarification of the proposed model's granular data access control mechanism. Employing Ethereum smart contracts, immutable logs, and trusted events, the model achieves its objectives effectively. It facilitates the sharing of patient data with authorized third parties, while significantly reducing the risk of data leakage and unauthorized access. This feature proves advantageous, particularly in identifying infectiously positive patients and helping users avoid contact with them.

Fig 1 illustrates the system diagram for the proposed model, depicting the process flow wherein the patient submits a sample to the testing center. Subsequently, the testing result is published and stored on the blockchain using a fog node. The subsequent operational processes of the system are clarified in the following subsections, providing a comprehensive overview of the system's functionality and workflow.

Initialization and registration. When third-party users, such as those from the education department, require access to patient data within the system, they must undergo a registration process. This involves submitting their credentials, including affiliation and EA. For example, if a third-party user belongs to the education department, they specify their affiliation, triggering the generation of a unique session key known as the Requester ID (RID). The RID serves as evidence of the user's registration and inclusion in the list of third-party users associated with the relevant sector, ensuring streamlined access control. The RID has a predetermined expiration period (θ), ensuring security and access control within the system. This study assumes a sufficient validity period for at least one complete access request cycle, though, the system architecture can be adjusted accordingly.

Algorithm 1 outlines the procedure for registering a third-party user within the system. Initially, the user initiates the process by sending a request message to join the network, accompanied by their public key (RBK_i) via the gateway. The validity of this message is verified by checking the freshness of its timestamp, as depicted in line 3 of the algorithm. Upon validation, the user's RBK_i is mapped to the corresponding administrator ($Gateway_{id}$) as illustrated in line

5. Consequently, a new RID (RID_i) is generated for the third-party user, as depicted in line 6. This RID serves as the key for the third-party user to engage with the network during subsequent interactions related to patient data access.

This streamlined registration and initialization process ensures the secure integration of third-party users into the system, facilitating efficient and controlled access to patient data while upholding data security and confidentiality protocols.

Algorithm 1: Third party user registration

Input RBK_i, $Gateway_{id}$, $Timestamp$

Output RID_i

Start

1 ***If*** $Current.Timestamp > Timestamp$ ***Do***

2 ***For*** *all* RBK_i *received* ***Do***

3 *Map* RBK_i *to* $Gateway_{id}$

4 $RID_i = hash\ (RBK_i, Gateway_{id})$

5 ***End For***

6 *Return* RID_i

7 ***End If***

End

Classification mechanism. The role-based classification mechanism, outlined in Algorithm 2, plays a crucial role in the proposed model's access control system. Upon receiving an access request, the classification function within the system retrieves the third-party user's request type (*RType*) and Requester ID (*RID*). This process is facilitated by maintaining a registry that stores and identifies each third-party user's entry in the system.

Algorithm 2 efficiently categorizes incoming requests based on their types. For each identified request type, the algorithm generates an index list that associates the correct request with its corresponding request number. This systematic approach, as demonstrated in lines 9–12, 13–16, and 17–22 of Algorithm 2, streamlines the process and enhances the system's responsiveness.

Once third-party users are successfully added to the system, they are classified according to their specific roles or purposes for accessing patient data. This classification ensures that each user is granted access only to data attributes relevant to their designated role. For instance, users affiliated with the education department are authorized to access and retrieve data attributes pertinent to the education sector exclusively. Conversely, access to data attributes outside their designated field is restricted.

Furthermore, certain attributes, such as ID card numbers or infectious disease test results, are designated as accessible to all users. This ensures the availability of critical information to relevant stakeholders while maintaining the integrity and security of sensitive data.

Overall, the role-based classification mechanism, coupled with granular access control, not only enhances data security but also facilitates efficient data management within the proposed model. This approach ensures that access to patient data is regulated, aligning with privacy regulations and promoting responsible data usage practices.

Algorithm 2: Classification

Input: Entire list of requests ($List_n$)

Output: Lists for different request types ($List_{edu}$, $List_{travel}$, $List_{health}$), $IndexList_i$

Start

1 **Initialize Lists:** Initialize $List_{edu}$, $List_{travel}$, and $List_{health}$ to store requests based on their types.

2 **Begin** Classification:

3 Iterate through **each** request **in** $List_n$.

4 Based **on** the request type ($RType_i$):

5 ***If*** $RType_i$ is Educational ***Then***

6 Add the request to $List_{edu}$.

7 Count the number of requests and update $IndexList_{edu}$.

8 Send $IndexList_{edu}$ to the patient.

9 ***Else If*** $RType_i$ is Traveling ***Then***

10 Add the request to $List_{travel}$.

11 Count the number of requests and update $IndexList_{edu}$.

12 Send $IndexList_{travel}$ to the patient.

13 ***Else*** ($RType_i$ is Health)

14 Add the request to $List_{health}$.

15 Count the number of requests and update $IndexList_{health}$.

16 Send $IndexList_{health}$ to the patient.

17 ***If*** all requests have been processed, **exit** the **loop**.

18 **Stop** Classification: **If** no more requests are received, **stop** the classification process.

End

Verification, granting access & revoking access. Algorithm 3 serves as the foundation for verifying the legitimacy of a requester within the system framework. It employs a validation mechanism where the RID_i is authenticated against the system's records. If the RID_i matches the hash generated from the requester's public key and the gateway ID (as detailed in line 5 of Algorithm 3), the request is deemed valid, indicating that the third-party user is duly registered within the network. Conversely, a mismatch leads to the request being tagged as invalid, signaling an unauthorized attempt to access the system.

Algorithm 3: Verification

Input RBK_i, $Gateway_{id}$, *Timestamp*

Output *Verification Status*

Start

1 *Request received* = ***True***

2 ***While*** *Request received* = ***True***

3 ***If*** $RID_i = hash\ (RBK_i, Gateway_{id})$ **Then**

4 *Return "Valid* RID_i*"*

5 ***Else***

6 ***Return*** *"Invalid* RID_i*"*

7 ***End If***

8 *Request received* = ***False*** *// Assuming condition to exit loop*

End

Building upon the verification process, Algorithm 4 outlines the protocol for authorizing access to data owned by the patient. The crux of this algorithm lies in matching the *RID* against the index list ($IndexList_i$), as elucidated in its operational steps. A successful match validates the request, affirming that it originates from a recognized third-party user. Should the *RID* fail to find a corresponding entry in the index list, the request is invalidated (referenced in the conditional checks of the algorithm). Following the validation of a request, the algorithm further evaluates if the request falls within the designated access timeframe. Access is consequently sanctioned only upon satisfying both the validation of the request and the temporal constraints.

Algorithm 4: Granting Access

Access time = ***True***;

Function *GrantAccess*()

Start

1 ***For*** $Request_i$ *in* $List_i$ *where i can be travel,health or educational*

2 ***If*** $RID_i \in request_i$ *&* $request_i \in IndexList_i$ ***Then***

3 ***Return*** *"Valid request for* $RType_i, RID_i$

4 ***Else***

5 ***Return*** *"Invalid request"*

6 ***End If***

7 ***If*** *Access time* = ***True Then***

8 ***Return*** *"Access granted"*

9 ***Else***

10 ***Return*** *"Access denied due to time restriction"*

11 ***End For***

End

Algorithm 5 introduces the capability to revoke previously granted access, enhancing the system's security and flexibility. The revocation process is initiated based on specific criteria,

such as the expiration of access time or the absence of the RID_i in the request queue, thereby terminating the access rights.

Algorithm 5: Revoking access

Input: Access time, RID_i, $request_i$

Output: Access Termination Status

Start

```
Function RevokeAccess()
    If Access time = False Then
        Return "Terminate access due to time restriction"
    Else If RID_i not in request_i Then
        Return "Terminate access due to invalid request ID"
    Else
        Return "Access not appropriate for termination"
    End If
```

End

The interplay of these algorithms ensures a robust mechanism for the classification, verification, and management of access rights within the system. Fig 2 encapsulates this procedural workflow, illustrating the seamless interaction between the third-party users and the data owners. Through the presentation and verification of the *RID*, patients can ascertain the authenticity and authorization of third-party requests. This verification empowers patients to grant access selectively, based on the third-party's affiliation, thereby safeguarding the privacy and integrity of the patient's records stored within the data repository.

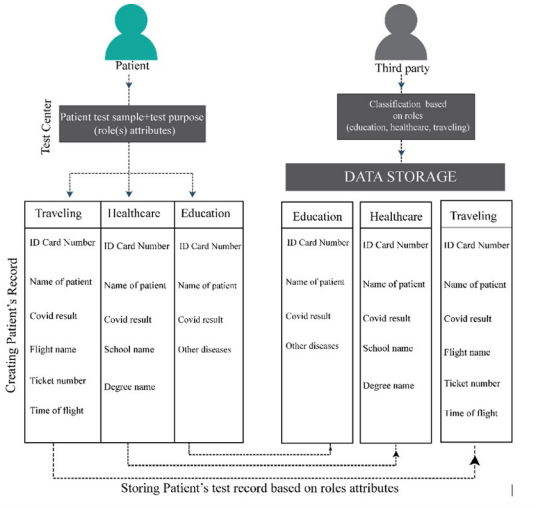

Fig 2. Role based classification.

https://doi.org/10.1371/journal.pone.0310407.g002

Attribute-based data confidentiality scheme

Blockchain storage is often decentralized and transparent, enabling unrestricted public access. Every transaction conducted on the blockchain is transparent and accessible to all participants in the system. For instance, when the system stores user data in the public ledger, transmits it to a third-party user, or verifies its authenticity, it becomes accessible to the participants. Hence, data stored on the blockchain needs to be obscured, and the unencrypted content should only be available to authorized entities.

Thus, this section presents a data confidentiality technique that aims to conceal users' information while it is being stored or sent by using public key infrastructure (PKI). To achieve this, the following postulations are provided:

***Postulation 1*:** Given two multiplicative cyclic groups $\mathcal{G}'$ and $\mathcal{G}''$ of prime order $\mathcal{p}$, such that 1D4BD is the generator of $\mathcal{G}'$. If m is a bilinear map function, then bilinear map pairing m: $\mathcal{G}' \times \mathcal{G}' \rightarrow \mathcal{G}''$ will have the following characteristics:

a. $m(x^s, y^t) = m(x, y)^{st}$, For all $x,y \in \mathcal{G}'$ and $s, t, w \in \mathbb{Z}_p$ (bilinearity).

b. Bilinear Mapping of m: $m(x,y) \neq 1$ (non-degeneracy).

c. $\mathcal{G}'$ is considered as a bilinear group if the operation of group in $\mathcal{G}'$ along with the bilinear map m (x,y) $x,y \in \mathcal{G}'$ are effectively computed (computability).

***Postulation 2*:** Let $A_{atr} = \{a_1. \ldots . .,a_N\}$ be set of attributes, $\ni \forall a_i \in A_{atr}$, $U = \{a_1. \ldots . .,a_q\}$ and $AS = \{a_1. \ldots . .,a_r\}$, where U and AS represents attribute list of users and access structures, respectively. Thus, if $U = AS$, this implies that U satisfies AS, i.e., $U_i = AS_i$, where $i = 1,2,. . .,n$.

***Postulation 3*:** Given a Decisional Parallel Bilinear Diffie-Hellman Exponent (DBDH) [63], having an actor $\mathcal{Q}$ with advantage $\mathcal{T}$ in solving the DBDH problem in $\mathcal{G}'$, any challenger with random values such as $s, t, w \in \mathbb{Z}_p$ with a DBDH challenge $\{(h,h^s,h^t,h^w,W)\}$ can determine if $\mathcal{W} = m(h, h)^{stw}$. Thus, the DBDH postulate holds if no polynomial time process has an insignificant benefit of at least $\mathcal{T}$ when addressing the decisional DBDH challenge in $\mathcal{G}'$ [64].

The following subsections describes processes involve in developing and sharing of the session key as well as encryption and decryption processes.

Setup: In this process a security parameter γ is taken as an input, while the output is given as: Public key (K_{pub}) and master key (M_k). From Postulation-1 assumes that some random elements and exponent $h_2, \varphi_1, \varphi_2 \in \mathcal{G}'$ and $\varepsilon \in \mathbb{Z}_{\mathcal{p}}$ were chosen this implies that $h_1 = h^{\epsilon}$ and $Z = m(h_2,h_1)$ can be achieved. Hence, the public is generated as: $K_{pub} = (\varphi_1,\varphi_2,h,h_2,h_1,Z)$ while the master key is generated as $E_k = h_2^{\varepsilon}$.

Key generation: In this process, the private key (K_{prv}) is generated using the master key (M_K), public key (K_{pub}) and set of attributes (AS). Thus, by choosing a random value, $\delta \in \mathbb{Z}_{\mathcal{p}}$, the private key is generated as: $K_{prv} = Gen_{key}(M_K,K_{pub},AS)$, and published as K_{prv}: $E_1 = h^{\delta}$, $E_2 = h_2^{\varepsilon}\left(\varphi_1, \prod_{a_{j\in U}} h_1^{a_j}\right)^{\delta}$, where $j = 1,2,. . .,n$.

Encryption: The inputs to this process include, the public key (K_{pub}), data Ð = {RID,ϑ}, and access structure AS, thus, the encrypted text, TK, is given as: $\mathrm{TK} = \mathrm{Encrypt}\left(K_{pub}, Ð, \mathrm{AS}\right)$, where ϑ represents other vital information associated with patient or third-party user. It initially chooses a random value $\sigma \in \mathbb{Z}_{\mathcal{p}}$, then computes $t' = \mathcal{h}^{\sigma}$, $t'' = Ð$. $\mathcal{h}^{\sigma}$, $t' = \left(\varphi_1, \prod_{a_{i\in AS}} h_1^{a_i}\right)^{\sigma}$ and $t'''' = \left(h_2, \varphi_2\right)^{\sigma}$. Hence, the encrypted text is published as: $TK = (AS \cdot t' \cdot t^{''} \cdot t' \cdot t'''')$**Decryption:** To generate the data Ð, the inputs to this process will

include, the public key (K_{pub}), the private K_{prv}, and the encrypted text TK: $Đ = Decrypt\left(\mathcal{K}_{pub}, TK, \mathcal{K}_{prv}\right)$. In this method, the encrypted text TK can only be deciphered by users who acquires the list of attributes U that satisfy the list of access structure AS. That is to say, if U satisfies AS, then the original message (M) can be recovered from the encrypted text, TK, as given in Eq 1 below:

$$Đ = \frac{m(E_1, t') \cdot t^{''}}{m(t', E_2)} = Đ \cdot \frac{m\left[(h_1, h_2)^{\sigma} \cdot \left(\varphi_1 \Pi_{a_{i\in U}} h_1^{a_i}, h\right)^{\delta\sigma}\right]}{m\left[\left(\begin{smallmatrix}\varepsilon \\ ,h_2\end{smallmatrix}\right) \cdot \left(\varphi_1 \Pi_{a_{j\in AS}} h_{1j}^{a\delta}\right)^{\delta}, h^{\sigma}\right)}] \quad (1)$$

Security analysis

This section provides evidence that the proposed scheme is secure using game theory approaches. The section begins by demonstrating that the granular data access control mechanism is protected under the real-or-random (ROR) model. The second part demonstrate that the attribute-based data confidentiality scheme is secure against an adversary who poses a significant threat to decisional DBDH.

Security proof for a granular data access control mechanism using ROR model

Each third party is classified as qualified or unqualified for data access based on their responsibilities in the proposed model. The patient uses the third party's session key to determine if the third party belongs to the role that allows data access, and then decides whether to grant or deny the third party's request. From Fig 1, the proposed system S has considered three users U_y, which are third-party U_{y1U}, gateway (admin) U_{y2G}, Patient U_{y3P}. These are instances y1, y2 and y3 for U, G and P. The adversary $\mathcal{A}$ can use the session key from the pool of session keys to pretend to be a qualified third party and tries to access the patients' data by executing various functions in the game model, these includes:

- The adversary may run the function $E\left(U_{y1U}, U_{y2G}, U_{y3P}\right)$ to eavesdrop on the transmitted messages over a public channel between U, G, and P.
- The adversary may execute the function $J(U_{y1U})$ to extract sensitive data from the user's device U.
- The adversary may run the function $K(U_y)$ to reveal the current session key between U_{y1U} and U_{y3P}. If the adversary is not able to expose the session key between $U_{\_y1U}$ and U_{y3P} using the $K(U_y)$ function, then the session key is secure.
- The adversary may execute the function $L(U_y\ and\ M)$, to send the message M to (U_y) and receive a response message.
- Before the game begins, the adversary executes a function $T(U_y)$ to get a fair coin f_c throw, with the outcome known only to $\mathcal{A}$. $\mathcal{A}$ makes a judgment on the test inquiry based on this outcome. If $\mathcal{A}$ runs the function and the session key is not from the pool and is new, then U_y returns the session key for $f_c = 1$ or a random number for $f_c = 0$. Otherwise, it will return null ($\perp$).

Following the test function's execution on U_y, $\mathcal{A}$ must differentiate the result value. $\mathcal{A}$ examines the random bit fc's reliability using the result of the test function. When the guessed

bit $f_c' = f_c$,$\mathcal{A}$ wins the game. Furthermore, each member of the system has access to a collision-resistant cryptographic one-way hash function *hf*(.). Similarly, *hf*(.) is considered as a random oracle in the proposed paradigm, Hash. Using Zipf's law model [65, 66], the following theorem is proposed:

Theorem 1. Given that $\mathcal{A}$ is capable of breaching the proposed model's session key security, and the benefit of $\mathcal{A}$ running in polynomial time is denoted by $ADV\mathcal{A}$. Then,

$$ADV\mathcal{A} \leq \frac{a_h^2 f}{|Hash|} + 2\{B.a_{send}^u\} \tag{2}$$

where a_{hf} is the number of hash values, |hash| is the volume of the hash function *hf* (.), and a_{send} is the number of send functions. In addition, *B and u* are the Zipf's parameters.

***Proof*:** We demonstrate the security of the session key using a series of the proposed games KM_I, where $I \in [0,3]$. $Vict_{AI}$ denotes the case in which $\mathcal{A}$ wins KM_I, by correctly predicting the random bit f_c. $Ur[Vict_A,KM_I]$ denotes the advantage of $\mathcal{A}$ winning the game KM_I. Each game is described in detail below.

***KM*$_0$:** This game enables $\mathcal{A}$ to conduct a real-world attack against the proposed model. At the start of KM_0, $\mathcal{A}$ selects a random bit f_c. Then, in accordance with this game, Eq 3 is obtained.

$$ADV\mathcal{A} = |2Mr\left[Vict_{\mathcal{A},KM_0}\right] - 1| \tag{3}$$

***KM*$_1$:** $\mathcal{A}$ executes the function $E\left(U_{y1U}, \cdot U_{y2G}; U_{y3P}\right)$ in this game and listens on the sent messages. Then, $\mathcal{A}$ executes $K(U_y)$ and $T(U_y)$ functions to verify that the derived session key is real or fake. To derive the session key the $\mathcal{A}$ should know the identities of U, G and P. As a result, there are no such cases in which $\mathcal{A}$ boosts ***KM*$_1$**'s likelihood of winning. As a result, ***KM*$_0$** and ***KM*$_1$** are vague, and the following result is obtained in Eq 4.

$$Mr\left[Vict_{\mathcal{A},KM_1}\right] = Mr\left[Vict_{\mathcal{A},KM_0}\right] \tag{4}$$

***KM*$_2$** In this game, $\mathcal{A}$ runs hash and send functions to retrieve the session key. By changing conveyed communications, $\mathcal{A}$ may launch an active attack. All exchanged messages, on the other hand, are created using secret credentials and random numbers and are safeguarded using the one-way hash function *hf*(.). Additionally, $\mathcal{A}$ makes it difficult to extract secret credentials and random nonces due to the fact that it is a computationally infeasible task according to the feature of *hf*(.). As a consequence of using the birthday paradox [67], we get the following conclusion.

$$|Mr\left[Vict_{\mathcal{A},KM_2}\right] - Mr\left[Vict_{\mathcal{A},KM_1}\right]| \leq \frac{a_{hf}^2}{2\mid Hash \mid} \tag{5}$$

***KM*$_3$** Here, the adversary may try to access the session key by executing the function *J* (U_{y1U}) and can extract private values such as password and username, which are stored in the device of the user. However, $\mathcal{A}$ has no knowledge of these values and, thus, cannot derive any secrete knowledge further. Additionally, it is computationally infeasible for $\mathcal{A}$ to estimate both password and username concurrently. In conclusion, ***KM*$_2$** and ***KM*$_3$** are literally identical. The following result can be reached by using Zipf's law.

$$|Mr\left[Vict_{\mathcal{A},KM_3}\right] - Mr\left[Vict_{\mathcal{A},KM_2}\right]| \leq B \cdot q_{send}^u \tag{6}$$

Assuming that all games have been completed, $\mathcal{A}$ must predict the bit in order to win the

game. As a consequence, the following result is obtained.

$$Mr\left[Vict_{\mathcal{A},KM_3}\right] = \frac{1}{2} \tag{7}$$

Using Eqs (1) and (2), the following result, Eq 8.

$$\frac{1}{2}ADV\mathcal{A} = |Mr \cdot \left[Vict_{\mathcal{A},KM_0} - \frac{1}{2}\right] = \left[Vict_{\mathcal{A},KM_1} - \frac{1}{2}\right]|. \tag{8}$$

Then, Eq (9) is derived using Eqs (7) and (8).

$$\frac{1}{2}ADV\mathcal{A} = |Mr \cdot \left[Vict_{\mathcal{A},KM_1} - \frac{1}{2}\right] = \left[Vict_{\mathcal{A},KM_3} - \frac{1}{2}\right]|. \tag{9}$$

With Eqs (6), (7), (8) and (9), the following conclusion using the triangle inequality can be obtained.

$$\frac{1}{2}ADV\mathcal{A} =| Mr\left[Vict_{\mathcal{A},KM_1}\right] - Mr\left[Vict_{\mathcal{A},KM_3}\right] \leq Mr\left[Vict_{\mathcal{A},KM_1}\right] - Mr\left[Vict_{\mathcal{A},KM_2}\right] +$$

$$Mr\left[Vict_{\mathcal{A}_{\mathcal{A},KM_2}}\right] - Mr\left[Vict_{\mathcal{A},KM_3}\right] \leq \frac{a_{hf}^2}{2 \mid Hash \mid} + B.\ a_{send}^u \tag{10}$$

By multiplying both sides of Eq (10) with 2, the required results can be displayed as follow:

$$ADV\mathcal{A} \leq \frac{a_{hf}^2}{\mid Hash \mid} + 2\left\{B \cdot a_{send}^u\right\} \tag{11}$$

Hence, theorem is proved.

Security proof for attribute-based data confidentiality scheme

Theorem 2: If the decisional DBDH challenge can be thwarted, an adversary-using actor may be able to circumvent it with a significant benefit.

Proof: Assuming that an adversary $\mathcal{A}$ with random values $s,t,w \in \mathbb{Z}_p$ with a DBDH challenge $\{(h,h^s,h^t,h^w,W)\}$ can challenge the proposed scheme with an $\mathcal{T}$ advantage, an actor $\mathcal{Q}$ can be created to play the DBDH game with $T/2$ advantage. Then to determine $\mathcal{W}$, if $W = m(h, h)^{stw}$, $\mathcal{Q}$ generate 1, otherwise, 0. The proof is further explained in five steps as follows:

Step-1: $\mathcal{A}$ chooses AS' and a challenge attribute set U' and then submit it to $\mathcal{Q}$, such that $\exists$ a' $\in$ U' that satisfies U' to AS'.

Step-2: $\mathcal{Q}$ chooses the random values $\eta,\rho \in \mathbb{Z}_p$ and assign the following parameters: $h_1 = h^{\epsilon}$, $h_2 = h^s$, $\varphi_1 = h^{\eta}\prod_{a_{i\in AS'}} h_1^{-a_i'}$, $\varphi_2 = h^{\rho} \cdot h_1^{-1}$, $Z = m(h_2,h_1) = m(h,h)^{st}$. Then $\mathcal{Q}$ generates $K_{pub} = (\varphi_1,\varphi_2,h,h_2,h_1,Z)$ and then submit it to $\mathcal{A}$.

Step-3: $\mathcal{A}$ ensures if $U \neq AS$', U' $\neq U$, otherwise, $\mathcal{Q}$ terminates the operation and randomly assumes the values. Thus, $\mathcal{Q}$ computes $\mathcal{K}_{prv}^{U'}$ as follows:

a. $\mathcal{Q}$ chooses a random value $\delta' \in \mathbb{Z}_p$, and generate $E_1' = h^{\delta'} \cdot h^{\frac{-1}{U-U'}}$, $E_2' = h_2^{\frac{-\eta}{U-U'}} \cdot \left(\varphi_1, \prod_{a_{j\in U}} h_1^{a_j}\right)^{\delta'}$.

b. $\mathcal{Q}$, then, submit the $\mathcal{K}_{prv}^{U'} = \left\{E_1', E_2'\right\}$ to $\mathcal{A}$.

From a, b above, if $\delta = \delta' - \frac{t}{U-U'}$, then, $\mathcal{K}_{prv}^{U'}$ is valid. That is:

$$E_1' = h^{\delta'} \cdot h_2^{\frac{-1}{U-U'}} = h^{\delta' - \frac{t}{U-U'}} = h^{\delta} \tag{12}$$

$$E_2' = h_2^{\frac{-\eta}{U-U'}} \cdot \left(\varphi_1, \prod\nolimits_{a_j \in U} h_1^{a_j}\right)^{\delta'} \tag{13}$$

Thus, by multiplying the value of E_2' with $(h^{st} \cdot h^{-st})$,

$$E_2' = h_2^{s} \cdot \left(\varphi_1, \prod_{a_j \in U} h_1^{a_j}\right)^{\delta} \tag{14}$$

Step-4: With this, $\mathcal{A}$ submits the data messages Đ′ and Đ″ to Q whom then tosses a fair binary coin $\omega \in \{0,1\}$, then, creates $\mathrm{TK}' = (\mathcal{D}_{\omega}, h^{w}, \mathcal{W}, (h^{w})^{\eta}, (h^{w})^{\rho})$. If $W = m(h,h)^{stw}$, then TK' is a valid encrypted text. If $\mathcal{W}$ is a random value in $\mathcal{G}'$ then $\mathcal{A}$ will assume that *TK*' and ω are two separate values.

Step-5: As $\mathcal{Q}$ act precisely as expected in Step-3, thus $\mathcal{A}$ performs a guess ω'. Q generate, 1 as its output only if $\omega' = \omega$. Hence, the probability P of thwarting the DBDH challenge can be deduced as follow:

$$P[\omega' = \omega] - 1/2 = P[\omega' = \omega \mid \omega = 0] \cdot P[\omega = 0] + P[\omega' = \omega \mid \omega = 1] \cdot P[\omega = 1] - 1/2 = \mathcal{T}/2 (15)$$

Experimental results and evaluation

This section delves into the simulation environment and the performance metrics employed in the development and assessment of the proposed model. The section outlines the framework within which the model was tested, highlighting the technical parameters and methodologies that underpin the simulation process. The evaluation of the proposed model is critically examined in comparison with existing models, specifically those introduced by H.R. Hasan et al. [21] and H. Saidi et al. (DSMAC) [57], as referenced in the study. The rationale for selecting these particular models for comparison is grounded in their relevance and the feasibility of comparing their performance and outcomes with those of the proposed model within similar operational contexts.

To clarify the advancements in security and operational efficiency achieved by the proposed model, a detailed comparative security and operational analysis is provided. This analysis not only benchmarks the proposed model against the aforementioned models but also highlights the innovative aspects of security enhancements and operational efficiencies it introduces. By drawing these comparisons, the analysis aims to underscore the contributions of the proposed model to the field and its potential to address existing gaps in the literature.

Furthermore, this section also presents a reflective discussion on the limitations encountered during the study and proposes avenues for future research and improvements. Acknowledging the limitations provides a balanced view of the proposed model's capabilities and areas where further enhancements are needed. It sets the stage for subsequent research efforts to build on the foundation laid by this study, aiming for advancements that could address the

identified limitations and potentially introduce new features or optimizations. This forward-looking perspective is crucial for the continuous evolution of the model and its applicability to real-world scenarios.

Design and implementation of smart contracts in PatCen

The PatCen system designs and executes smart contracts to automate and robustly enforce data access rules in a secure and transparent manner within the blockchain framework. Solidity, a specialized high-level programming language, implements these contracts on the Ethereum blockchain. The following is a comprehensive examination of the design logic, inherent self-triggering characteristics, and execution procedure of these smart contracts.

Design Logic and Self-Triggering Mechanism: PatCen specifically engineers the smart contracts to manage a range of functions, such as data access requests, permission assessment, and transaction recording on the blockchain. The fundamental principle of these contracts is to guarantee that only specifically authorized users may retrieve confidential healthcare information, in accordance with their predetermined responsibilities and permissions. The contracts offer self-triggering capabilities, designed to initiate automatically when specific conditions, like a user's submission of an access request, are satisfied.

Execution within the Blockchain Environment: When smart contracts are deployed on the Ethereum blockchain, they undergo decentralized execution. Following a user's submission of a transaction, such as an access request, the relevant smart contract autonomously executes the request in accordance with the predetermined logic. The contract authenticates the user's role and assesses if the request satisfies the specified criteria for access. If the specified requirements are satisfied, the contract records the transaction on the blockchain, ensuring the transparency and immutability of all actions.

Stack of technology in PatCen

The PatCen system employs a robust technological stack that enables the blockchain-based data management framework to function securely and effectively. The following is a comprehensive summary of the primary technologies employed:

Ethereum blockchain: PatCen is based on the Ethereum blockchain, a well-known and established system that provides strong smart contract functionality. The permissioned network architecture of Ethereum is well-suited for healthcare applications, where ensuring data security and implementing limited access are of utmost importance. The inherent decentralized structure of the blockchain guarantees the safe and immutable recording of all transactions and data access events, thus establishing a robust foundation of trust and accountability.

Solidity: Solidity serves as the primary programming language for creating the PatCen smart contracts. The programming language was purposefully developed to facilitate the creation of contracts that are executed on the Ethereum Virtual Machine (EVM). The syntax of Solidity bears resemblance to that of JavaScript, making it easily comprehensible for developers while nevertheless offering robust functionalities for implementing complex logic within smart contracts. The selection of Solidity guarantees that the contracts exhibit both efficiency and security, using inherent measures to mitigate prevalent vulnerabilities.

Metamask: Metamask serves as a software tool to manage Ethereum accounts and streamline interactions with the public blockchain. The technology functions as an intermediary between the user's web browser and the Ethereum network, facilitating the safe management of private keys, transaction signing, and interaction with the PatCen system. The integration of Metamask facilitates convenient system access for users, enabling them to safeguard their credentials and data while retaining appropriate control.

Web3.js: The Web3.js library is a JavaScript framework that enables seamless communication between the front-end application and the Ethereum blockchain. This functionality enables the PatCen system to execute transactions, engage with smart contracts, and extract data from the blockchain. The Web3.js framework facilitates a smooth connection between the user interface and the blockchain backend, hence allowing instantaneous updates and interactivity inside the decentralized ecosystem.

Implementation setup

In the development of the proposed model, we utilized Python and Solidity programming languages for their robustness and compatibility with blockchain technologies. The deployment and storage of Ethereum were facilitated through the Metamask Ethereum client, showcasing the practical application of the model within the Ethereum blockchain environment. Our experimental setup was conducted on the Rinkeby testnet, employing a Proof of Authority (POA) consensus mechanism to validate transactions efficiently and securely, which is critical for maintaining the integrity and reliability of the blockchain operations.

The construction of the model's logic and the interactions with smart contracts were orchestrated using the Web3.py Python library alongside other relevant modules. This approach enabled precise and efficient communication between the model and the Ethereum blockchain, ensuring seamless execution of operations within the blockchain environment.

The experimental simulations were carried out on personal computers equipped with an AMD PRO A8-9600B R5, 10 COMPUTE CORES 4C+6G, operating at 2.40 GHz, providing a stable and controlled environment for conducting the tests. This hardware setup was selected to ensure a balance between performance and accessibility, allowing the experiments to be replicable in environments accessible to most researchers.

In conducting these experiments, it was paramount to maintain a consistent setup across all test scenarios to avoid bias and ensure the reliability of our observations and results. By implementing the models in identical setup scenarios, we aimed to achieve the most accurate and unbiased comparison of their performances, thereby providing a solid foundation for evaluating the effectiveness and efficiency of the proposed model in a blockchain environment.

Experimental evaluations

In evaluating the performance and quality of any system, specific metrics are essential for providing a comprehensive assessment. Similarly, for the proposed system, a set of key performance indicators has been established to offer a holistic view of its efficiency and effectiveness. These metrics include:

- Cost Analysis: This metric examines the system's economic efficiency, focusing on gas consumption and associated gas prices. Understanding the financial implications of operating the system within a blockchain environment, where transactions and operations incur costs in the form of gas fees, is critical.
- Encryption and Decryption Times: These metrics assess the efficiency of the cryptographic processes within the system. The speed at which data can be securely encrypted and subsequently decrypted is vital for evaluating the system's performance in protecting sensitive information while ensuring accessibility for authorized users.
- Key Generation Time: The time required to generate secure cryptographic keys is another critical performance indicator. This metric provides insights into the efficiency of the system's security mechanisms, specifically in the context of generating robust keys that underpin the overall security of the cryptographic processes.

- Computational Latencies: This metric measures the delay or latency in processing operations within the system. Lower computational latencies are indicative of a more responsive and efficient system, which is especially important in applications requiring real-time or near-real-time processing capabilities.
- Computational Throughput: This metric evaluates the system's ability to process a high volume of operations within a given time frame. Higher computational throughput indicates a system's capacity to handle larger loads efficiently, making it a crucial metric for assessing scalability and performance under varying conditions.

Together, these metrics provide a comprehensive framework for evaluating the proposed system's performance, offering insights into its operational efficiency, security, and cost-effectiveness. This approach ensures a balanced evaluation, taking into account both the technical and economic aspects of the system's operation.

Cost analysis

The Remix environment represents a pioneering method for meticulously documenting the financial intricacies of transactions within the Ethereum network. In this innovative approach, every log entry comprehensively encapsulates the expenses associated with transactions and executions. A crucial aspect of navigating this ecosystem is understanding the transaction speeds, which are intricately tied to gas pricing, predominantly denoted in Gwei (gas price). Smart contract development necessitates a meticulous assessment of gas costs to preempt any potential ancillary expenditures. It's worth noting that miners tend to prioritize transactions with higher Gwei values, thus enhancing the likelihood of processing transactions with elevated Gwei prices.

Various factors, including loops, arrays, mappings, variable storage, and data types, profoundly influence transaction costs. The paramount concern lies in the practicality and efficiency of the solution. As such, our proposed methodology capitalizes on the inherent immutability of the blockchain, leveraging events and logs instead of on-chain storage.

While the price of gas may fluctuate depending on the day and time of year, our methodology has been rigorously evaluated during non-peak periods, specifically in June 2021, when the costs associated with executing and transacting operations are relatively lower. On June 25, 2021, the ETH Gas Station recorded gas prices of 15.1, 15.1, 5.7, and 5.7 Gwei for the fastest, fast, average, and lowest categories, respectively. Table 3 provides a detailed cost analysis in United States dollars (USD) based on the average gas price of 5.7 Gwei.

Table 3 elucidates the transaction costs and execution expenses denominated in Gwei. Notably, the adduser function incurs a maximum cost of $0.1855. While this price is considered modest, it emerges as the most expensive among all functions within our proposed system. The adduser function serves a pivotal role in facilitating user addition and classification based on their responsibilities within the system. Despite its relatively higher cost, the absence of loops or arrays in the methods suggests that the anticipated expenses remain inconsequential.

In comparison, our proposed approach boasts an average cost of $0.1395 per full program execution, while the benchmark model [21] demonstrates an average cost of $0.16375, based on the gas price at ETH Gas Station on June 25, 2021. The results shown in Fig 3 show that our proposed approach cuts computing costs by a large amount compared to the average execution and transaction costs in the benchmark models. These margin disparities highlight our methodology's efficacy and cost-efficiency.

Table 3. Cost analysis table.

Function name	Transaction Cost	Execution Cost	Cost USD
addpatient	22409	2391	$0.1325
adduser	31357	3849	$0.1855
grantaccess	23549	2297	$0.1375
deleteuser	20349	2033	$0.121
deletepatient	20702	2067	$0.121

Average cost: $ 0.1395

https://doi.org/10.1371/journal.pone.0310407.t003

In terms of gas consumption per access request and grant, Fig 3 shows that the proposed model is much less sensitive to more interactions with third-party users than benchmark models. The deliberate avoidance of the clustering approach, which demands extensive computational efforts in smart contract development, accounts for this. Furthermore, our model demonstrates a decrease in transaction overhead as third-party users increase, leading to a notable reduction of around 46 percent in total block time validation, as reported by Etherscan.

Encryption, decryption & key generation latencies

The core concept hinges on the interaction between a myriad of third-party users and the retrieval of specific patient records within the system. This model delves into an average of twenty (20) interactions between third-party users and patients to scrutinize their dynamics. Central to the model's operation is the access structure, where an upsurge in third-party user requests corresponds to a proportional increase in the system's time allocation. Our study quantifies the average time overhead across three key performance metrics—encryption, decryption, and key generation—analyzing them individually based on the frequency of interactions with third-party users within the system.

The system intricately links temporal costs to the volume of interactions with third-party users. Figs 4–6 delineate the correlation between the model's encryption, decryption, and key generation time, and the frequency of interactions with third-party users. Notably, as the

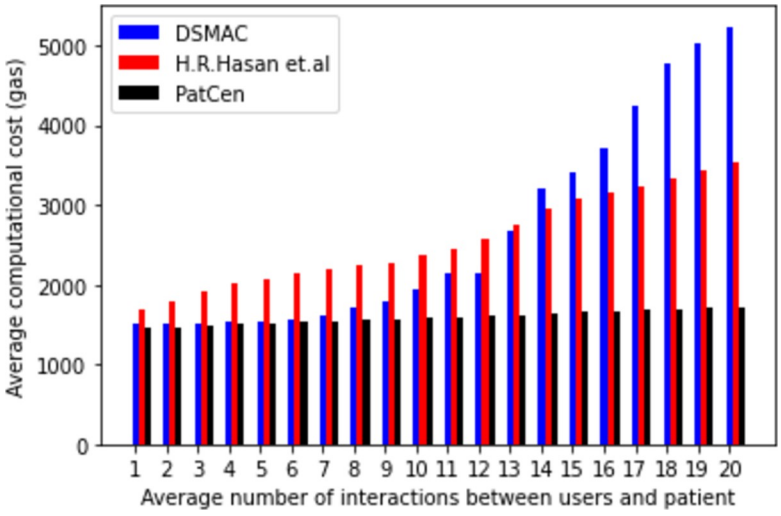

Fig 3. Average computational cost (execution and transaction costs).

https://doi.org/10.1371/journal.pone.0310407.g003

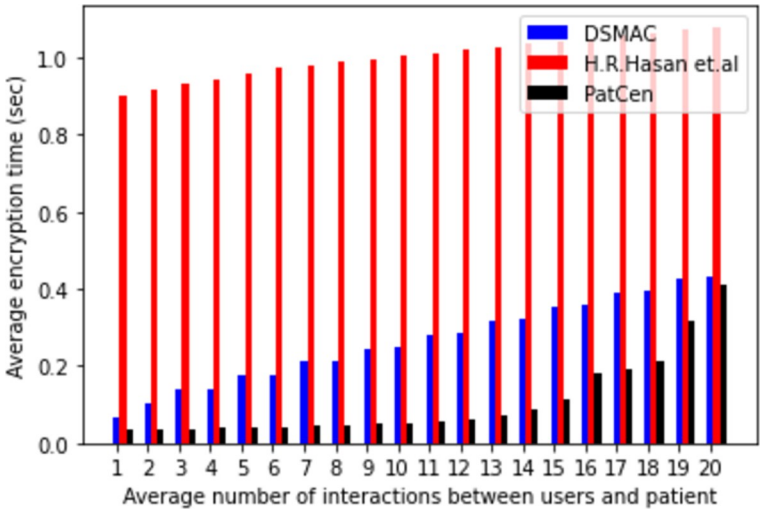

Fig 4. Average encryption time.

https://doi.org/10.1371/journal.pone.0310407.g004

number of interactions escalates, so does the time required for encryption, decryption, and key creation. Our proposed framework demonstrates average times of 0.036805556, 0.050916667, and 0.062111111 for encryption, decryption, and key generation, respectively. In contrast, the model by H.R. Hasan et al. exhibits times of 0.416, 0.2825, and 0.227 for the same operations, while the DSMAC model showcases times of 0.263629408, 0.65823956, and 0.235203387, respectively.

Moreover, our findings underscore a positive correlation between time passage and the number of interactions across all models. However, the proposed model evinces a minimal and consistent rise in time compared to both base models, particularly under heightened interaction volumes. Conversely, the benchmark models exhibit a substantial increase in overhead as interactions surge. Notably, the proposed model's overhead remains consistently low and stable under moderate interaction volumes, a stark contrast to the benchmark models.

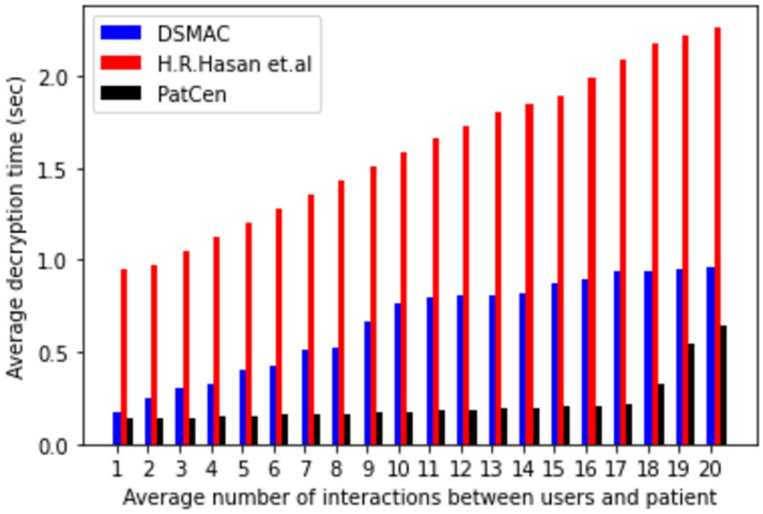

Fig 5. Average decryption time.

https://doi.org/10.1371/journal.pone.0310407.g005

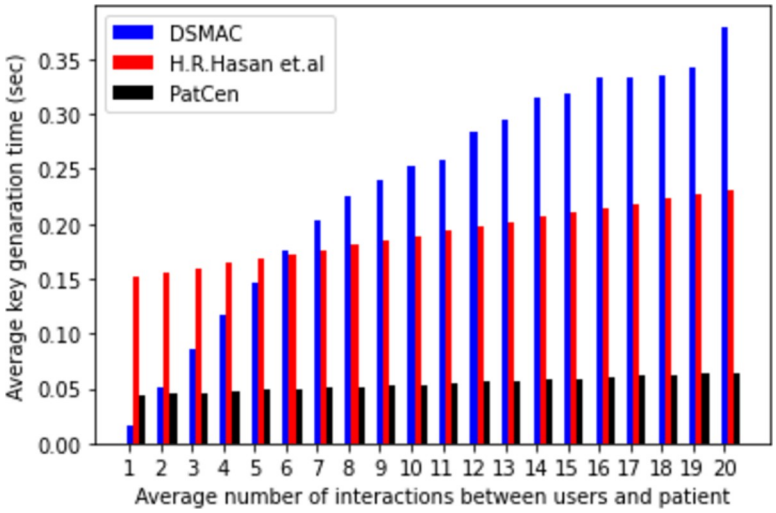

Fig 6. Average key generation time.

https://doi.org/10.1371/journal.pone.0310407.g006

The volatility observed in the benchmarks is attributed to the utilization of POW consensus and the implementation of extensive encryption and decryption processes by the central administration. In contrast, our proposed model employs the POA consensus mechanism, which contributes to its enhanced efficiency in access control. Based on our analysis of computational overhead and time duration, it is evident that our proposed model outperforms benchmark models in terms of both access request and grant time for patient test data, showcasing a higher level of efficiency.

Computational latency and throughput

Computational latency, in this context, signifies the time elapsed from the submission of a transaction by a user to its processing and recording in the ledger. The meticulous monitoring, documentation, and comparison of computational latency serve to gauge its performance relative to benchmark models. Our assessment of transaction latency performance employed a background timer program operating concurrently with transaction executions, with time measurement determined by the system processor clock, contingent upon the prevailing processor schedule.

The model we propose demonstrates reduced computational latency, as evidenced by the data in Fig 7, compared to benchmark models. A consistent increase in average computational latency is observed with the escalation of users' interactions across all models. However, the average latency exhibited by our proposed PatCen model is notably reduced compared to that seen in the benchmark models. This reduced delay can be attributed to the implementation of the proof-of-authority consensus mechanism. It is noteworthy that there exists an inverse relationship between security level and latency, whereby higher security is associated with lower latency.

The PatCen model has the potential for a significant influx of access requests, primarily due to the diverse range of interactions with third-party users that require management and processing. Computational throughput was evaluated by measuring computing overhead per unit of gas consumption during the progressive increase in user interactions. Subsequently, we compared the average computational throughput of our proposed model with that of benchmark models.

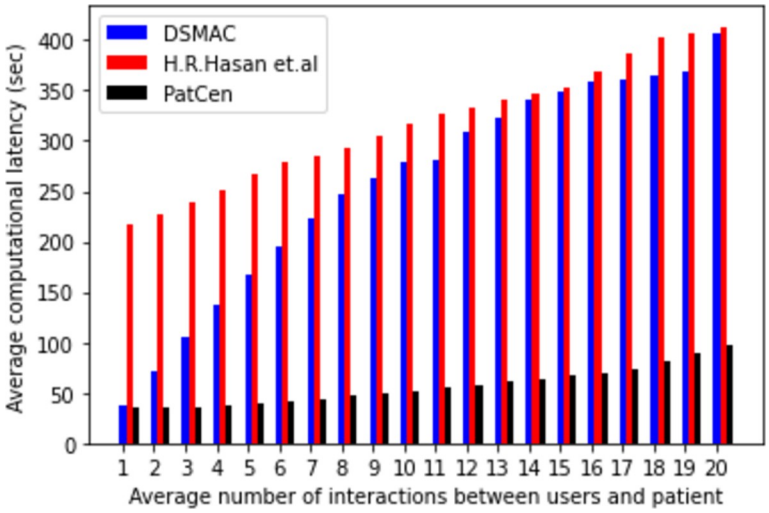

Fig 7. Average computational latency.

https://doi.org/10.1371/journal.pone.0310407.g007

Initially, both the proposed scheme and the DSMAC model exhibit comparable throughputs. However, the extensive encryption and decryption procedures conducted by the central administration in the DSMAC and H.R. Hasan et al. methods throughout various stages of credential verification and query processing consistently alter the ledger's state, resulting in lower throughput compared to the PatCen model.

Fig 8 illustrates a significant decline in the throughput of both DSMAC and H.R. Hasan et al. models as the number of users' interactions grows. Therefore, we can deduce that the proposed PatCen model outperforms benchmark models in terms of effectiveness and efficiency.

Comparative security and operational analysis

Table 4 provides a comprehensive comparative analysis of the security and operational aspects between the proposed PatCen protocol and two existing schemes developed by H.R. Hasan et al. [21] and H. Saidi et al. (DSMAC) [57]. The assessment categorized system performance using "Yes" and "No" indicators to signify the extent to which each system fulfilled the evaluated security and operational criteria.

The analysis reveals that the systems presented in references [21, 57] lack session key security and fine-grained data access during data transfers, as highlighted in the table. Specifically, the benchmark systems [21, 57] failed to ensure the confidentiality of third-party users, particularly concerning user anonymity within the system. Furthermore, this study shows that the methods used in the benchmark systems have higher computing overhead, lower throughput, and higher latencies, thereby falling short in delivering enhanced security and efficiency within the system.

In contrast, the PatCen model successfully satisfied all security and operational requirements considered in this study. This underscores the efficacy and robustness of the proposed model in meeting the stringent demands of security and operational excellence within the system.

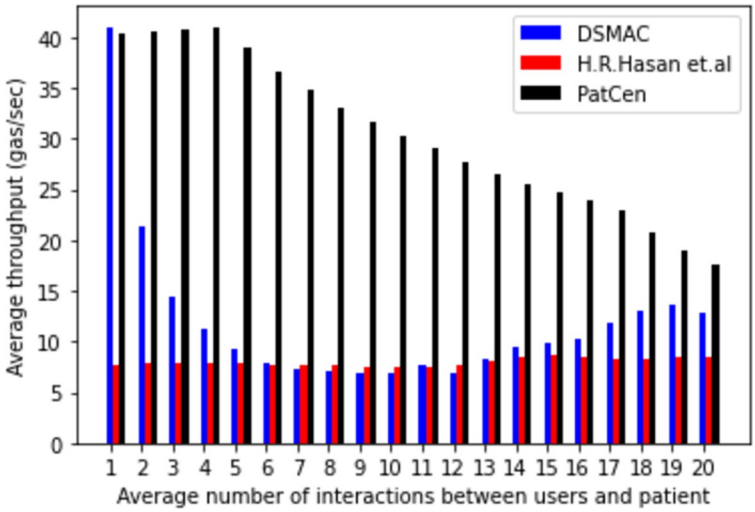

Fig 8. Average computational throughput.

https://doi.org/10.1371/journal.pone.0310407.g008

Justification for the superior performance of the PatCen model

The superior performance of the PatCen model compared to existing methods can be attributed to several key innovations and optimizations that directly address the unique challenges associated with managing infectious disease test records in a healthcare setting. These advancements ensure that PatCen not only meets but exceeds the requirements for security, efficiency, and scalability, which are critical in this context.

Granular data access control

The PatCen model employs a granular data access control mechanism that is more advanced than the traditional role-based access controls used in other methods. This mechanism allows for fine-tuned permissions, enabling patients to precisely manage who can access their data and under what circumstances. This level of control is essential in healthcare, where data privacy and patient autonomy are paramount.

- **Impact:** The enhanced control over data access reduces the risk of unauthorized access and ensures that only necessary information is shared with third parties, improving both security and compliance with privacy regulations such as GDPR and HIPAA. Other methods, which often use broader access control schemes, may not provide the same level of protection or flexibility, leading to potential privacy risks and inefficiencies.

Table 4. Security and operational comparison.

Security Features	DSMAC [57]	H.R. Hasan et al. [21]	PatCen
User registration	Yes	Yes	Yes
User validation	Yes	No	Yes
Session key security	No	No	Yes
Considering patient privileges	Yes	Yes	Yes
Fine grain data access	No	No	Yes
User anonymity	No	No	Yes
Patient privacy	Yes	No	Yes

https://doi.org/10.1371/journal.pone.0310407.t004

Optimized blockchain framework with PoA consensus

PatCen's use of a permissioned blockchain with a Proof-of-Authority (PoA) consensus mechanism is a significant improvement over more traditional consensus methods like Proof-of-Work (PoW) or Proof-of-Stake (PoS). The PoA mechanism is specifically designed for environments where the network participants are known and trusted, which is typical in healthcare networks.

- **Impact:** This approach significantly reduces computational overhead and enhances transaction speed, making the system more efficient and scalable. In contrast, other models that rely on PoW or PoS may experience higher costs and slower performance, particularly in large-scale implementations, which can limit their practical applicability in real-time healthcare scenarios.

Game-theoretic security enhancements

A distinctive feature of the PatCen model is its integration of game theory to enhance security. By modelling the interactions between the system and potential adversaries, PatCen can anticipate and mitigate security threats more effectively than traditional static security measures.

- **Impact:** This proactive security strategy ensures that the system remains resilient against evolving threats, providing a higher level of data protection. Other methods, which may not incorporate such dynamic security approaches, could be more vulnerable to new types of attacks, leading to potential data breaches and compromised patient information.

Scalability and real-time performance

The PatCen model is designed with scalability in mind, ensuring that it can handle a growing number of users and transactions without a decline in performance. The system's architecture supports high throughput and low latency, which are critical for applications that require real-time access to healthcare data, such as during emergency medical situations or when rapid verification of test results is needed for travel.

- **Impact:** The ability to maintain performance as the system scales is a major advantage over other methods that may struggle with increased load, leading to bottlenecks and slower response times. This makes PatCen more suitable for widespread deployment in diverse healthcare environments.

In conclusion, the PatCen model's superior performance is the result of its innovative approach to data access control, optimized blockchain framework, advanced security measures, and scalability. These features directly address the limitations of existing methods, making PatCen a more effective and reliable solution for managing infectious disease test records in healthcare settings. By overcoming the drawbacks of traditional models, PatCen ensures that healthcare data is managed securely, efficiently, and in a manner that respects patient autonomy and privacy.

Discussions

In this section, we provide an in-depth examination of the PatCen model, exploring its underlying mechanisms, compliance with ethical and regulatory standards, and the potential limitations and future directions of the system. We begin by discussing the PoA consensus

mechanism and its role in ensuring the efficiency, security, and performance of the PatCen blockchain. Following this, we address how the model aligns with critical regulatory frameworks such as GDPR and HIPAA, highlighting the specific measures implemented to protect patient data and ensure compliance with legal requirements. Additionally, we evaluate the limitations of the proposed model, particularly in relation to scalability and the reliance on the Ethereum blockchain, and outline our vision for future improvements. This discussion provides a holistic view of the strengths and areas for enhancement within the PatCen system, setting the stage for ongoing research and development in the field of blockchain-based healthcare solutions.

Proof-of-Authority (PoA) consensus mechanism in PatCen

The PoA consensus method is an essential element of the PatCen system, guaranteeing efficient and safe functioning within our permissioned blockchain framework. PoA is particularly well-suited for healthcare environments because the network members, such as hospitals, labs, and healthcare providers, are established and reliable institutions. This technique provides several benefits that are well-suited to the needs of handling confidential health information.

1. Efficiency and Reduced Processing Demands: In contrast to PoW or PoS systems that require substantial processing resources and energy use, PoA functions effectively with minimum computational expenses. Validators in a PoA system are pre-approved and recognized by the network, which means there is no need for complex cryptographic puzzles or large stake holdings. To maintain low operating expenses, healthcare settings require rapid and reliable data processing efficiency.
2. Centralized Control with Identified Validators: In a PoA blockchain, a trusted select few validators are responsible for confirming transactions and appending them to the blockchain. These validators are typically organizations or individuals that have a recognized authority within the network, such as healthcare institutions or regulatory authorities. The centralized management of the system strengthens security by guaranteeing that only authorized and reputable entities have the authority to verify transactions. Additionally, it lessens the probability of malicious behaviour by holding validators accountable for their actions and enabling easy detection and auditing.
3. Contribution to Security and Performance: The PoA mechanism plays an important role in enhancing the PatCen system's security and functionality. The system mitigates the danger of unauthorized access or tampering with patient data by imposing restrictions on the number of validators and confirming their credibility. In addition, the efficient validation procedure allows for quicker transaction times and increased throughput, guaranteeing real-time accessibility to healthcare data, which is vital in times of public health crises.

Overall, the PoA consensus process is very suitable for the specific requirements of a healthcare-oriented blockchain such as PatCen. It offers a harmonious combination of efficiency, security, and performance, making it a perfect option for handling the delicate and time-sensitive data that is inherent in healthcare systems.

Alignment with ethical standards and regulatory frameworks

The PatCen system specifically adheres to the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) to ensure compliance with ethical standards and regulatory frameworks, which are essential for safeguarding healthcare data from unauthorized access and misuse. The implementation of this alignment

guarantees that the system not only safeguards patient confidentiality but also adheres to legal obligations pertaining to the management of personal health data.

Adherence to the GDPR. The GDPR is an all-encompassing regulatory framework that oversees the handling of personal data within the European Union. PatCen's design aligns with the GDPR's fundamental principles, namely data minimization, obtaining permission, and the right to access and erase personal data.

Data Minimization: PatCen implements stringent measures to ensure that only the essential data is collected and processed. The system implements a granular access control mechanism that restricts access to specific data characteristics based on the user's role and the request's context. This methodology effectively mitigates the potential vulnerability of sensitive information, thereby reducing the likelihood of illegal intrusion.

Consent Management: The system integrates procedures to acquire and oversee patient permission prior to engaging in any data processing operations. The GDPR outlines explicit and informed permission mandates that allow patients to revoke their authorization at any given moment.

Right to Access and Erasure: PatCen protects patients' legal rights to access their data and request its deletion. Patients can access their records and configure access rights through the system's user interface. In the event that a patient communicates a desire for data deletion, the system guarantees the secure erasure of all pertinent data from the blockchain, upholding the "right to be forgotten" as mandated by the GDPR.

Adherence to HIPAA. HIPAA establishes the minimum requirements for safeguarding confidential patient information inside the United States. We have developed the PatCen system to incorporate functionalities that align with the data privacy and security regulations outlined by HIPAA. These features specifically focus on ensuring the protection of electronic protected health information (ePHI).

Data Security: PatCen employs strong encryption techniques to protect ePHI during storage and transmission. This measure ensures the preservation of health information confidentiality and security, thereby reducing the risk of unauthorized access and breaches. The use of blockchain technology serves to augment security measures by providing an unalterable log of all data transfers, a crucial aspect for ensuring auditability and adherence to the security regulations set out by HIPAA.

Access Control: PatCen's access control measures guarantee that only those with permission may access ePHI, in compliance with HIPAA's privacy guidelines. The enforcement of role-based access restrictions inside the system is facilitated by smart contracts, which dynamically configure permissions according to the user's role and the particular data they are authorized to access.

Auditability: In order to comply with HIPAA's standards for auditing and accountability, PatCen offers a thorough audit trail of all data access and change activities. The inherent characteristics of transparency and immutability in blockchain technology guarantee the recording of all operations and prevent any alterations, thus establishing a reliable framework for monitoring and tracing data handling activities.

In conclusion, PatCen ensures the appropriate handling of sensitive healthcare data by adhering to GDPR and HIPAA, thereby upholding patient privacy and complying with international regulatory requirements. The design of the system places significant emphasis on the elements of data security, consent management, and secure access, establishing it as a resilient solution for the administration of health information in a manner that adheres to legal requirements and ethical principles.

Limitations and future improvements

In the healthcare sector, the integration of blockchain technology is steadily gaining traction owing to its prowess in enhancing data security, integrity, and accessibility. This paper introduces the PatCen model, a secure framework tailored for implementing granular access control for infectious disease test information. Leveraging blockchain technology, the PatCen concept fortifies security measures. Its decentralized architecture safeguards against tampering or illicit modifications, thereby upholding the integrity of critical health data. Transparency among all participants in the blockchain network is ensured, while access control mechanisms facilitate secure data sharing with authorized entities. Furthermore, the utilization of smart contracts and distributed consensus techniques fosters trust among stakeholders in the healthcare domain.

However, the model's effectiveness in expansive and dynamic environments may be limited by its constrained experimental framework and reliance on the Ethereum blockchain for storage and processing. The current state and future advancements of the Ethereum network could impact the scalability and efficacy of the approach. Consequently, our future endeavors will prioritize scalability as a primary objective while simultaneously safeguarding both patient and user privacy rights.

Future investigations will broaden the scope of the model to encompass various forms of access-related threats. Researching deeper into anonymity and privacy, as pivotal components, will be imperative to adeptly address any unforeseen challenges that may arise. Moreover, further exploration will be conducted to evaluate the model's potential for application in tangible devices. Additionally, forthcoming work will provide detailed insights to enhance understanding, including specific features of the mobile application and the user interface for granting access. These components collectively empower patients to confer privileges upon other users.

Conclusion

The objective of this study is to analyze the conceptualization, implementation, and assessment of a blockchain-driven access control mechanism for electronic health records. The proposed system facilitates the generation of records for tests linked to infectious diseases, the storage of patient data, and the implementation of access restrictions to ensure that only authorized users, based on their respective roles, may access the data. In this study, both the data and the session key are encrypted to ensure that unauthorized users are unable to access the data by abusing the session key of another user's computer. The proposed solution underwent an evaluation of its methodologies, which included a full cost analysis, encryption and decryption processes, key production, as well as measures of latencies and throughput. The results of the security study indicate that the proposed solution demonstrates safety within the framework of the DBDH game theory and successfully attains session key security according to the ROR formal security analysis game theory, among other notable results. The simulation results demonstrate that the proposed approach exhibits reduced computational cost, increased throughput, and decreased latencies in comparison to the benchmark models. The cryptographic simulation results demonstrate that the proposed model exhibits significantly enhanced security and efficiency compared to the benchmark model. The proposed approach aims to mitigate the spread of infectious diseases by effectively collecting, managing, and securely disseminating time-sensitive data to authorized users with the explicit consent of the patients involved.

Author Contributions

Conceptualization: Bello Musa Yakubu, Syeda Mahera Ali.

Data curation: Bello Musa Yakubu, Syeda Mahera Ali.

Formal analysis: Bello Musa Yakubu, Syeda Mahera Ali.

Funding acquisition: Bello Musa Yakubu, Pattarasinee Bhattarakosol.

Investigation: Bello Musa Yakubu, Syeda Mahera Ali.

Methodology: Bello Musa Yakubu, Syeda Mahera Ali.

Project administration: Majid Iqbal Khan, Pattarasinee Bhattarakosol.

Resources: Majid Iqbal Khan, Pattarasinee Bhattarakosol.

Software: Bello Musa Yakubu, Syeda Mahera Ali.

Supervision: Majid Iqbal Khan, Pattarasinee Bhattarakosol.

Validation: Bello Musa Yakubu, Majid Iqbal Khan.

Visualization: Majid Iqbal Khan, Pattarasinee Bhattarakosol.

Writing – original draft: Bello Musa Yakubu, Syeda Mahera Ali.

Writing – review & editing: Majid Iqbal Khan, Pattarasinee Bhattarakosol.

References

1. Mahase E. Covid-19: Mental health consequences of pandemic need urgent research, paper advises. BMJ. 2020. https://doi.org/10.1136/bmj.m1515 PMID: 32299806
2. Aftab A, Musa Yakubu B, Mushtaq A, Shafique A. Psychological Effects of COVID-19 on Mental Health: An ICT-based Perspective. Merit Research Journal of Business and Management. 2022. https://doi.org/10.5281/zenodo.6287621
3. Mahapatra B, Bhorekar KK. Analyzing the Economic Depression Post-COVID-19 Using Big Data Analytics. Studies in Systems, Decision and Control. 2021. https://doi.org/10.1007/978-3-030-60039-6_16
4. Chamola V, Hassija V, Gupta V, Guizani M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. IEEE Access. 2020; 8. https://doi.org/10.1109/ACCESS.2020.2992341
5. Shams SA, Haleem A, Javaid M. Analyzing COVID-19 pandemic for unequal distribution of tests, identified cases, deaths, and fatality rates in the top 18 countries. Diabetes and Metabolic Syndrome: Clinical Research and Reviews. 2020; 14. https://doi.org/10.1016/j.dsx.2020.06.051 PMID: 32604014
6. Choi Y, Kim JS, Choi H, Lee H, Lee CH. Assessment of social distancing for controlling covid-19 in korea: An age-structured modeling approach. Int J Environ Res Public Health. 2020; 17. https://doi.org/10.3390/ijerph17207474 PMID: 33066581
7. Karthik V, Rani L, Brundha MP. COVID-19 spread through petting-a review. International Journal of Current Research and Review. 2020. https://doi.org/10.31782/IJCRR.2020.SP38
8. Worldometer. Coronavirus Incubation Period. Feb.22.2020. 2020. Available from: https://www.worldometers.info/coronavirus/coronavirus-incubation-period/
9. Marbouh D, Abbasi T, Maasmi F, Omar IA, Debe MS, Salah K, et al. Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. Arabian Journal for Science and Engineering. 2020. https://doi.org/10.1007/s13369-020-04950-4 PMID: 33072472
10. Altaf A, Iqbal F, Latif R, Yakubu BM, Latif S, Samiullah H. A Survey of Blockchain Technology: Architecture, Applied Domains, Platforms, and Security Threats. Soc Sci Comput Rev. 2022. https://doi.org/10.1177/08944393221110148
11. Sookhak M, Jabbarpour MR, Safa NS, Yu FR. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications. 2021. https://doi.org/10.1016/j.jnca.2020.102950
12. Hyla T, Pejaś J. eHealth integrity model based on permissioned blockchain. Future Internet. 2019; 11. https://doi.org/10.3390/fi11030076
13. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access. 2017; 5. https://doi.org/10.1109/ACCESS.2017.2730843

14. Hirtan L, Krawiec P, Dobre C, Batalla JM. Blockchain-based approach for e-health data access management with privacy protection. IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD. 2019. https://doi.org/10.1109/CAMAD.2019.8858469

15. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020; 50. https://doi.org/10.1016/j.jisa.2019.102407

16. Neudecker T, Hartenstein H. Network layer aspects of permissionless blockchains. IEEE Communications Surveys and Tutorials. 2019; 21. https://doi.org/10.1109/COMST.2018.2852480

17. Ziar RA, Irfanullah S, Khan WU, Salam A. Privacy Preservation for On-Chain Data in the Permission less Blockchain using Symmetric Key Encryption and Smart Contract. Mehran University Research Journal of Engineering and Technology. 2021; 40. https://doi.org/10.22581/muet1982.2102.05

18. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016; 40. https://doi.org/10.1007/s10916-016-0574-6 PMID: 27565509

19. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, et al. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. 2018 IEEE Globecom Workshops, GC Wkshps 2018—Proceedings. 2019. https://doi.org/10.1109/GLOCOMW.2018.8644088

20. An J, Gall F Le, Kim J, Yun J, Hwang J, Bauer M, et al. Toward global IoT-enabled smart cities interworking using adaptive semantic adapter. IEEE Internet Things J. 2019;6. doi:10.1109/JIOT.2019.2905275

21. Hasan HR, Salah K, Jayaraman R, Arshad J, Yaqoob I, Omar M, et al. Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates. IEEE Access. 2020; 8: 222093–222108. https://doi.org/10.1109/ACCESS.2020.3043350 PMID: 34812373

22. Uddin MdA, Stranieri A, Gondal I, Balasubramanian V. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. Blockchain: Research and Applications. 2021; 100006. doi:10.1016/j.bcra.2021.100006

23. Wang J, Han K, Alexandridis A, Chen Z, Zilic Z, Pang Y, et al. A blockchain-based eHealthcare system interoperating with WBANs. Future Generation Computer Systems. 2020; 110. https://doi.org/10.1016/j.future.2019.09.049

24. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information (Switzerland). 2017; 8. https://doi.org/10.3390/info8020044

25. Thalhammer F, Schöttle P, Janetschek M, Ploder C. Blockchain Use Cases Against Climate Destruction. Cloud Computing and Data Science. 2022. https://doi.org/10.37256/ccds.3220221277

26. Namasudra S, Deka GC. Introduction of DNA Computing in Cryptography. Advances of DNA Computing in Cryptography. 2018. https://doi.org/10.1201/9781351011419-1

27. Datta S, Namasudra S. Blockchain-Based Smart Contract Model for Securing Healthcare Transactions by Using Consumer Electronics and Mobile Edge Computing. IEEE Transactions on Consumer Electronics. 2024. https://doi.org/10.1109/TCE.2024.3357115

28. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences (Switzerland). 2019; 9. https://doi.org/10.3390/app9091736

29. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. Proceedings—2016 2nd International Conference on Open and Big Data, OBD 2016. 2016. https://doi.org/10.1109/OBD.2016.11

30. Hongwei L, Xinhui W, Sanyang L. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. Optim Methods Softw. 2004; 19.

31. Gan C, Saini A, Zhu Q, Xiang Y, Zhang Z. Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor. Multimed Tools Appl. 2020. https://doi.org/10.1007/s11042-020-09322-6

32. Kish LJ, Topol EJ. Unpatients-why patients should own their medical data. Nature Biotechnology. 2015. https://doi.org/10.1038/nbt.3340 PMID: 26348958

33. Al Omar A, Rahman MS, Basu A, Kiyomoto S. MediBchain: A blockchain based privacy preserving platform for healthcare data. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. https://doi.org/10.1007/978-3-319-72395-2_49

34. Omar A Al, Bhuiyan MZA, Basu A, Kiyomoto S, Rahman MS. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Computer Systems. 2019;95. doi:10.1016/j.future.2018.12.044

35. Sahi MA, Abbas H, Saleem K, Yang X, Derhab A, Orgun MA, et al. Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. IEEE Access. 2017; 6. https://doi.org/10.1109/ACCESS.2017.2767561

36. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One. 2020; 15. https://doi.org/10.1371/journal.pone.0243043 PMID: 33296379

37. Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal. 2018. https://doi.org/10.1016/j.csbj.2018.06.003 PMID: 30069284

38. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc. 2018; 39. https://doi.org/10.1016/j.scs.2018.02.014

39. Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. International Conference on Advances in Biomedical Engineering, ICABME. 2017. https://doi.org/10.1109/ICABME.2017.8167555

40. Huang X. Blockchain in Healthcare: A Patient-Centered Model. Biomed J Sci Tech Res. 2019; 20. https://doi.org/10.26717/bjstr.2019.20.003448 PMID: 31565696

41. Guo H, Li W, Nejad M, Shen CC. Access control for electronic health records with hybrid blockchain-edge architecture. Proceedings—2019 2nd IEEE International Conference on Blockchain, Blockchain 2019. 2019. https://doi.org/10.1109/Blockchain.2019.00015

42. Chen Y, Ding S, Xu Z, Zheng H, Yang S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J Med Syst. 2018; 43. https://doi.org/10.1007/s10916-018-1121-4 PMID: 30467604

43. Tripathi G, Ahad MA, Paiva S. S2HS- A blockchain based approach for smart healthcare system. Healthcare. 2020; 8. https://doi.org/10.1016/j.hjdsi.2019.100391 PMID: 31753750

44. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst. 2018; 42. https://doi.org/10.1007/s10916-018-0982-x PMID: 29876661

45. Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics (Switzerland). 2020; 9. https://doi.org/10.3390/electronics9010094

46. Tao Q, Ding H, Jiang T, Cui X. B-DSPA: A Blockchain-Based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad Hoc Networks. IEEE Internet Things J. 2024; 11. https://doi.org/10.1109/JIOT.2023.3289057

47. Younis M, Lalouani W, Lasla N, Emokpae L, Abdallah M. Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. IEEE Syst J. 2022; 16. https://doi.org/10.1109/JSYST.2021.3092519

48. Javed L, Yakubu BM, Waleed M, Khaliq Z, Suleiman AB, Mato NG. BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution. International Journal of Electrical and Computer Engineering Research. 2022; 2. https://doi.org/10.53375/ijecer.2022.302

49. Ding Y, Sato H. Bloccess: Enabling Fine-Grained Access Control Based on Blockchain. Journal of Network and Systems Management. 2023; 31. https://doi.org/10.1007/s10922-022-09700-5

50. Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. IEEE Internet Things J. 2021; 8: 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

51. Egala BS, Pradhan AK, Dey P, Badarla V, Mohanty SP. Fortified-Chain 2.0: Intelligent Blockchain for Decentralized Smart Healthcare System. IEEE Internet Things J. 2023. https://doi.org/10.1109/JIOT.2023.3247452

52. Zhang G, Chen X, Zhang L, Feng B, Guo X, Liang J, et al. STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted Agricultural IoT Blockchain Terminal. International Journal of Interactive Multimedia and Artificial Intelligence. 2022; 7. https://doi.org/10.9781/ijimai.2022.07.004

53. Wu G, Wang S, Ning Z, Li J. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. IEEE Internet Things J. 2022; 9. https://doi.org/10.1109/JIOT.2021.3138104

54. Bigini G, Lattanzi E. Toward the InterPlanetary Health Layer for the Internet of Medical Things With Distributed Ledgers and Storages. IEEE Access. 2022; 10. https://doi.org/10.1109/ACCESS.2022.3196933

55. Sharma P, Namasudra S, Chilamkurti N, Kim BG, Gonzalez Crespo R. Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. ACM Trans Sens Netw. 2023; 19. https://doi.org/10.1145/3577926

56. Namasudra S, Sharma P. Achieving a Decentralized and Secure Cab Sharing System Using Blockchain Technology. IEEE Transactions on Intelligent Transportation Systems. 2023; 24. https://doi.org/10.1109/TITS.2022.3186361

57. Saidi H, Labraoui N, Ari AAA, Maglaras LA, Emati JHM. DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data. IEEE Access. 2022; 10. https://doi.org/10.1109/ACCESS.2022.3207803

58. George M, Chacko AM. Health Passport: A blockchain-based PHR-integrated self-sovereign identity system. Frontiers in Blockchain. 2023; 6. https://doi.org/10.3389/fbloc.2023.1075083

59. Gaur VS, Sharma V, McAllister J. Abusive adversarial agents and attack strategies in cyber-physical systems. CAAI Trans Intell Technol. 2023; 8: 149–165. https://doi.org/10.1049/cit2.12171

60. Zhang D, Shafiq M, Wang L, Srivastava G, Yin S. Privacy-preserving remote sensing images recognition based on limited visual cryptography. CAAI Trans Intell Technol. 2023; 8: 1166–1177. https://doi.org/10.1049/cit2.12164

61. Charles D. A Blockchain Cross-Border Payment System to Enable a Potential Caribbean Regional Emissions Trading Scheme. Green and Low-Carbon Economy. 2023. https://doi.org/10.47852/bonviewGLCE3202825

62. An M, Fan Q, Yu H, An B, Wu N, Zhao H, et al. Blockchain Technology Research and Application: A Literature Review and Future Trends. Journal of Data Science and Intelligent Systems. 2023. https://doi.org/10.47852/bonviewJDSIS32021403

63. Fugeng Z, Chunxiang X, Zeng F, Xu C. Attribute-based encryption with hidden threshold access structure. COMPUTER MODELLING & NEW TECHNOLOGIES. 2014. Available: www.cmnt.lv

64. Wang J, Zhu M, Li M, Sun Y, Tian Z. An Access Control Method Against Unauthorized and Non-compliant Behaviors of Real-time Data in Industrial IoT. IEEE Internet Things J. 2023. https://doi.org/10.1109/JIOT.2023.3285992

65. Powers DMW. Applications and Explanations of Zipf's Law. Proceedings of the Joint Conference on New Methods in Language Processing and Computational Natural Language Learning, NeMLaP/CoNLL 1998. 1998. https://doi.org/10.3115/1603899.1603924

66. Bochkarev V V., Lerner EY, Nikiforov AA, Pismenskiy AA. Finding exact constants in a Markov model of Zipfs law generation. Journal of Physics: Conference Series. 2017. doi:10.1088/1742-6596/936/1/012028

67. Suzuki K, Tonien D, Kurosawa K, Toyota K. Birthday paradox for multi-collisions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2008. https://doi.org/10.1093/ietfec/e91-a.1.39