Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2025.060143

ARTICLE

A Blockchain-Based Access Management System for Enhanced Patient Privacy and Secure Telehealth and Telemedicine Data

Ayoub Ghani[1,*], Ahmed Zinedine[1] and Mohammed El Mohajir[2]

[1]Faculty of Sciences, Sidi Mohammed Ben Abdellah University, Fez, 30000, Morocco

[2]Faculty of Sciences, Abdelmalek Essaadi University, Tetouan, 93030, Morocco

*Corresponding Author: Ayoub Ghani. Email: Ayoub.ghani@usmba.ac.ma

Received: 25 October 2024 Accepted: 23 December 2024 Published: 23 January 2025

ABSTRACT

The Internet of Things (IoT) advances allow healthcare providers to distantly gather and immediately analyze patient health data for diagnostic purposes via connected health devices. In a COVID-19-like pandemic, connected devices can mitigate virus spread and make essential information, such as respiratory patterns, available to healthcare professionals. However, these devices generate vast amounts of data, rendering them susceptible to privacy breaches, and data leaks. Blockchain technology is a robust solution to address these issues in telemedicine systems. This paper proposes a blockchain-based access management solution to enhance patient privacy and secure telehealth and telemedicine data. The paper seeks to contribute in two significant ways to the enhancement of patient privacy and security: firstly, by defining a patient-centric access mechanism that adheres to the General Data Protection Regulation (GDPR) and our security requirements, as well as describing architecture, all pertinent access management actions, and proposed smart contracts including their design goals; secondly, by formalizing and validating the security properties through the application of the SeMF security modeling framework as well as, performing the cost analysis. As a result, the SeMF has assessed the satisfaction of our security requirements, including data integrity, data authenticity, data confidentiality, and authentication. As a result, the system has proven alignment with defined security requirements. Furthermore, the implementation has demonstrated the cost savings of our system. Finally, the system has been compared to other solutions based on design goals and GDPR compliance. Thus, the system is suitable for enhancing patient security and privacy through a patient-centric approach.

KEYWORDS

Blockchain; IoT; SeMF; telemedicine

1 Introduction

Telehealth and telemedicine services have advanced as a result of the significant transformation of healthcare systems facilitated by the rise of connected devices supplied with biosensors (worn or incorporated) [1]. These devices can track various health metrics, such as glucose levels, blood pressure, pulse rate, respiratory rate and patterns.

Additionally, a categorization of these devices has been proposed in [2]: (cat. 1) Stationary Devices, utilized in hospitals; (cat. 2) Medical Embedded Devices, used and embedded inside the body; (cat. 3) Medical Wearable Devices, prescribed by doctors; and (cat. 4) Wearable Health Monitoring Devices, worn on the body. In addition, Telehealth and telemedicine advance treatment outcomes, care coordination, and accessibility to healthcare through the use of Internet of Things (IoT) technology. However, security and privacy are the main concerns of IoT devices due to their continuous internet connectivity and limited storage capacity. Consequently, patient data is at risk of privacy breaches, as evidenced by more than 40 major security breaches and privacy leakages worldwide three years ago, affecting well-known companies, including Microsoft as well as governmental institutions [3].

Current telehealth systems store data in centralized databases owned by healthcare providers, which results in significant privacy concerns, including unauthorized data access. Furthermore, centralized systems are prone to Single Point of Failure (SPoF), risking data loss due to hardware or system malfunctions. In the event of malicious attacks, alterations to patient data may go undetected and unrecoverable [4]. Access management also suffers from several drawbacks, including indefinite data access by third parties, limited trust in third parties, and challenges in conducting audit trails. Additionally, there is often a misunderstanding of access granted by users and additional data usage, highlighting the need for a human-centric approach that clarifies the objective for data usage [5].

The General Data Protection Regulation (GDPR), established by the European Union, provides a legal framework that enforces data protection guidelines and enhances consumer control over their personal data [6]. Security and privacy concerns require a patient-centric approach to improve the protection of patient data storage and sharing. This approach must also comply with GDPR regulations for access management and data-sharing processes.

Therefore, Blockchain technology can mitigate the security and privacy challenges facing telehealth and telemedicine. Additionally, Blockchain is a decentralized system where peer-to-peer transactions occur between parties that may not be trusted without the need for intermediaries. Users are involved in the verification and validation processes. Additionally, Blockchain offers strong security through cryptographic encryption, which ensures data confidentiality. It functions as a tamper-resistant distributed ledger made up of sequential blocks linked by hash values, recording transactions from public or private peer-to-peer networks [7]. Transaction data is hashed using Merkle trees to manage storage and access [8]. Consequently, blockchain data cannot be altered without affecting all subsequent blocks in the ledger [9]. Consensus algorithms are used to maintain data consistency across the distributed network.

Here are the main features that define blockchain technology:

- **Decentralization.** Seeks to end the need for a central authority to own and control the network.
- **Transparency.** Ensures that every record is visible to every node (This can be applicable to public Blockchain)
- **Persistency.** Validates transactions within minutes and instantly identifies invalid transactions, with no possibility of deleting or rolling back recorded ones.
- **Immutability.** Stores every recorded data permanently unless malicious users control the blockchain network.
- **Anonymity.** To conceal their identities, users interact using generated addresses in a public blockchain. Conversely, private blockchains require restricted user identification.

Additionally, the Ethereum blockchain [10] introduces the concept of Smart Contracts, which aims to enhance efficiency and lower costs. A Smart Contract serves the purpose of setting up the basic logic

over a decentralized application that allows people to send money, goods, or services to one another without trusting one another. Fig. 1 illustrates the smart contract lifecycle, which includes four stages: establishing predefined contract rules, triggering events, self-execution, and settlement. Furthermore, the Inter-Planetary File System (IPFS) [11] is a peer-to-peer distributed file system that connects all computers using a single file system. It offers decentralized storage. IPFS has a block store model with high throughput and content-addressed hyperlinks. Each file is given a distinctive hash that can be accessed by all network peers. Any modifications to the file lead to a corresponding change in the hash.

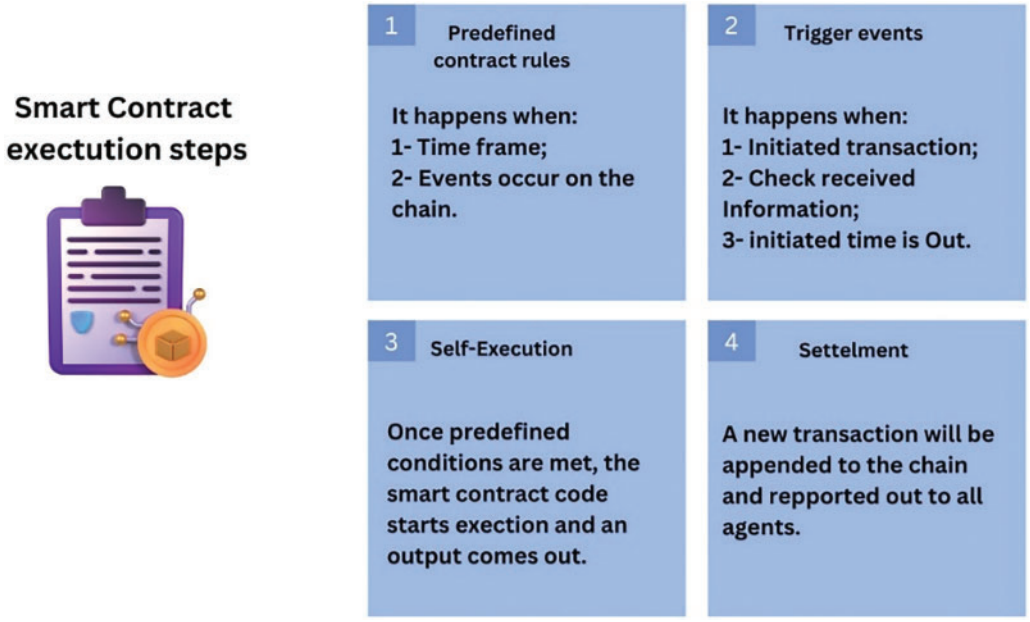

Figure 1: Smart contract lifecycle

In view of this, the paper proposes a blockchain-based access management system for telehealth and telemedicine. This system aims to enhance patient privacy and data security by recording every access to data on Blockchain. To evaluate the system's effectiveness in addressing privacy and security concerns, we plan to use a formal security modeling framework (SeMF).

The paper is organized as follows: Section 2 discusses related works and contributions. Section 3 provides an overview of blockchain technology. Section 4 defines the system requirements. Section 5 describes the proposed system, detailing its design and architecture, and includes all related actions presented in sequence diagrams and algorithms that automate the access process based on key characteristics of Blockchain. Section 6 covers the formalization and validation of the system's security properties. Finally, Section 7 presents the conclusion.

2 Related Works & Contributions

2.1 Related Works

Bawany et al. [12] conducted an in-depth analysis of the potential benefits and adaptability challenges associated with integrating blockchain technology into the telehealth sector. Their research aims to develop a comprehensive telehealth framework called BlockHeal that integrates essential

healthcare services using Blockchain to ensure privacy, security, and trust. By leveraging smart contracts, BlockHeal includes decentralized storage, secure data exchange, and various services like digital prescriptions, drug supply chain management, health insurance, and emergency services. Furthermore, Zhuang et al. [13] presented a thorough analysis of the significant enhancements that Blockchain brings to the exchange of healthcare data. They use Blockchain and smart contracts to ensure data security and data provenance and provide patients with control over their health records. They demonstrate the feasibility, stability, security, and robustness of the proposed model through a large-scale simulation, highlighting its potential to improve patient-centric data exchange. Furthermore, Sheela et al. [14] examined the significant effect of blockchain technology on the healthcare sector, especially regarding security and privacy. Their outcomes suggest that Blockchain can significantly improve data integrity by guaranteeing that health records remain accurate and unaltered. This technology ensures nonrepudiation, meaning when data is recorded, it cannot be denied, hence increasing trust in the system. At this level, Puneeth et al. [15] proposed a blockchain-based framework to secure Electronic Health Records (EHR) with patient-centric access control using smart contracts, integrating Blockchain's immutability and decentralization features with advanced cryptographic techniques. The framework uses a hybrid cryptographic algorithm for encryption and stores EHR data using off-chain storage known as InterPlanetary File System (IPFS). Furthermore, Boumezbeur et al. [16] proposed a blockchain-based framework for secure EHR sharing. The framework uses cryptographic techniques and smart contracts to manage access control and ensure data privacy. The framework shows efficient encryption and decryption times. It also ensures flexible access control by allowing patients to manage access to their health records. Nevertheless, the process for revoking access permissions might not be straightforward, potentially leading to unauthorized access if permissions are not updated. In addition, Tahir et al. [17] proposed a privacy-preserving and secure framework for sharing Electronic Health Records (EHRs) using blockchain technology. The framework leverages cryptographic techniques and smart contracts on the Ethereum blockchain to ensure secure storage and access control of EHRs. The system architecture includes three layers: data collecting, data storing, and data sharing, involving entities such as EHR owners, EHR users, cloud storage, and Blockchain. The framework aims to enhance data privacy, authenticity, integrity, confidentiality, flexible access control, and user authentication. However, the framework presents some limitations: access to data with unlimited time, automated user authentication without control from a legitimate authority, and no option to revoke authentication. Moreover, Shah et al. [18] proposed an e-healthcare management system using the Internet of Things (IoT) and blockchain technologies. This aims to provide comprehensive, reliable, and secure services for patients. It also tries to address the challenges of providing low-cost and high-quality medical services, especially in the context of global aging. However, as patients store EHR data in the system, there is a risk of data loss, which challenges data integrity. Further, Li et al. [19] proposed a secure data-sharing system for electronic health (eHealth) systems. The framework, named TrustHealth, leverages blockchain technology and Trusted Execution Environments (TEEs) to improve eHealth security by ensuring data privacy, authenticity, integrity, and confidentiality. While it provides robust user authentication and access control through smart contracts and cryptographic techniques, it faces challenges such as the complexity of key management and potential vulnerabilities in smart contract design. Moreover, Mao et al. [20] presented a blockchain-based platform designed to enhance the management and sharing of medical data. The platform aims to address the challenges of data authenticity, security, and traceability in the medical field. Smart contracts are used for trusted storage and data authenticity verification. They manage user access control with predefined rules. Although the paper emphasizes data security, it could benefit from the integration of advanced privacy-preserving techniques, such as homomorphic encryption or differential privacy.

Furthermore, numerous studies have explored the integration of blockchain technology with the Internet of Things (IoT) [21–25]. While these works highlight significant advancements and potential applications, they also reveal several limitations in terms of access control management, user authentication, data authenticity, and data ownership.

Furthermore, numerous research efforts have been undertaken to mitigate and address security and privacy-related issues within an Internet of Things environment through the application of blockchain technology, often referred to as Blockchain 4.0. For instance, Hameed et al. [26] present a comprehensive taxonomy of privacy and security requirements specifically adapted to Blockchain-based Industry 4.0 applications. They categorize these requirements into three distinct types: first, **Confidentiality, Integrity, and Availability Triad.** This one focuses on ensuring that data is kept confidential, remains unaltered, and is accessible when needed. Second, **the Authentication, Authorization, and Accounting Triad** is crucial for verifying the identities of users (authentication), determining their access rights (authorization), and keeping track of their activities (accounting). Third, **securing smart contracts** involves ensuring that they are free from vulnerabilities, function as intended, and cannot be tampered with. The integration of blockchain technology in IoT environments, as outlined in these categories, aims to create a more secure and trustworthy system. By addressing the CIA and AAA triads, along with securing smart contracts, Blockchain can significantly enhance the security and privacy of IoT applications. This approach not only protects data and ensures its integrity but also provides a transparent and accountable framework for managing access and interactions within the IoT ecosystem. Furthermore, our system will consider the above requirements to mitigate the aforementioned limitations in the literature. By incorporating advanced security measures, ensuring compliance with GDPR regulations, and leveraging Blockchain, we aim to enhance the privacy and security of patient data.

2.2 Contributions

This paper proposes an access management system that leverages blockchain technology. It aims to improve patient privacy and secure data within the telehealth and telemedicine sectors. The system seeks to record every single access to data in Blockchain, thereby providing patients with full control over their data and increased transparency regarding data sharing. With the General Data Protection Regulation (GDPR) in mind, this study aims to establish a patient-oriented system for access management. Moreover, the potential contributions of blockchain technology to the telehealth and telemedicine sectors motivate its application for dynamic access management. The characteristics of blockchain technology mitigate challenges in the existing systems. This suggested approach employs smart contracts for automating activities such as controlling access, identifying unallowed use, and adding or removing nodes from the system network based on their trustworthiness. The following section outlines the key enhancements that blockchain technology brings to our system:

- **Security.** Blockchain can guarantee patient data confidentiality and integrity, it also offers authenticity to data requestors.
- **Persistency.** Once access-related transactions are added to the Blockchain, they cannot be deleted or altered. Any blocks containing invalid access-related transactions can be instantly identified.
- **Immutability.** One of the most important aspects of blockchain technology is that it provides a record that cannot be altered and is time-stamped.
- **Transparency.** All access-related transactions are visible and auditable.
- **Smart contract.** It ensures the automatization of the access management process.

To ensure that our system solves the privacy and security issues, we proceed an evaluation process using formal security modeling framework (SeMF) [27], which is based on formal language theory. SeMF aims to validate the usability of our system to effectively address privacy and security issues. Moreover, SeMF stands for two main processes the formalization and the validation of the system's privacy and security properties.

Consequently, our work aims to provide two substantial contributions to the improvement of patient security and privacy, as follows:

1. This involves defining the proposed patient-centric access mechanism that satisfies the GDPR regulations and our security requirements, detailing the system's design and architecture, outlining all potential actions related to access management, and describing the proposed smart contracts, including their design goals.

2. This involves the formalization and validation of the system's privacy and security properties by applying the formal security modeling framework SeMF, performing the cost analysis, and comparing it with existing solutions.

3 Blockchain Overview

Blockchain consists of a series of blocks linked using unique hash values. Because of its decentralization, the system is not owned or controlled by a single entity. The key characteristics of blockchain technology include decentralization, transparency, persistence, immutability, and anonymity. Additionally, there are three types of Blockchain: permissionless, permissioned, and consortium. Permissionless enables anyone to join the network and have full access to stored records, while permissioned restricts access to data. The consortium is a hybrid solution between permissioned and permissionless, trusted and trustless networks. In a distributed system, a network of nodes uses consensus to validate and verify transactions in a conflict-free environment. In addition, the consensus is implemented using Lottery-based algorithms like Proof of Work (PoW) or Voted-based algorithms like Practical Byzantine Fault Tolerance (PBFT) [28]. Each approach is suitable for specific network dependencies. Lottery-based approaches involve lottery winners or miners broadcasting valid blocks to the network. This approach occasionally results in an unusual scenario if two lottery winners broadcast two valid blocks. The network will validate the longest chain [29]. On the other hand, voting-based approaches require the majority of nodes to validate transactions or blocks, providing low-latency finality but potentially compromising scalability and speed.

4 System Requirements

There are some security risks that come with telemedicine and telehealth systems. Our main concern is about how to manage access. In order to address this, the system needs to follow GDPR standards for managing access and data protection. Below, we provide a detailed explanation of the system requirements. Additionally, Table 1 presents the key notations used in this paper.

Table 1: Notations and decripription

Notation	Meaning
Di	Health-related data.
Ui	Patient who owns data.
ReFi	A unique number that refers to access.
Ri	Data requestor (i.e., Doctors, Hospitals, or Labs) who request access to access patient's data.
Pi	Purpose to accessing data Di.
Ni	Nature of data Di.
RA	The Regulatory Authority is known as the network governor (i.e., Healthcare Ministry).
Pki	User's public key.
Ski	User's private key.
Ai	The transaction performed by a user includes Di, as i refers to the index.
t	The period of time in which the access is valid.
λ	User's local view.
ω	A series of actions.
Γ	A list of actions.
P	All users in the system.
L	Set of banned users by RA.

4.1 Security

Ensuring security is a fundamental aspect of our system, as it is paramount for establishing and maintaining trustworthiness in the system. According to [26], the security requirements can be outlined here:

- **Confidentiality.** This is the key security requirement of any application or system designed to protect patient data Di from unauthorized access or potentially malicious users. In other respects, there is a potential risk of compromising patient privacy. Di may include identifiers, which are considered as sensitive information.
- **Integrity.** This feature guarantees the authenticity and reliability of Di, effectively preventing malicious users from tampering with stored Di in databases or communicating Di over the network. Furthermore, any Di received by a healthcare provider is equal to the Di provided by the patient.
- **Availability.** For instance, even in the case of a network attack, the system should sustain operation at the system level, and Di access at the transaction level can be made available to authorized users without failing, being inaccurate, or being distorted. In other words, the system should guarantee to users P access to resources, as well as Di involved in the process of performing actions A1, . . . , An.
- **Authentication.** This constitutes an initial security layer, as it prevents the identification of users P. Thus, each time a user1 performs an action A1, the sender's identity must be verified for user2 in order to safely receive A1 and other related D1.

- **Authorization.** This denotes that only authorized users are able to perform actions A1, . . . , An in the system. Moreover, it prevents unauthorized ones to perform actions A1, . . . , An or access Di which improves system security.
- **Nonrepudiation.** This requirement is essential for the system, ensuring that all users P cannot repudiate the sending or receiving of any action Ai.
- **Accountability.** This is a critical requirement for most blockchain-based systems because users can act as adversaries in the network and engage in fraudulent activities such as unauthorized access to critical data Di. Moreover, accountability enables Ui to monitor Ri, who accessed data Di unlawfully and reports it back to the Regulatory Authority RA. The authenticity and nonrepudiation can thus be proven through accountability.

In the upcoming section, the SeMF will formalize these security requirements in detail.

4.2 Privacy

To ensure compliance with the General Data Protection Regulation [6], our proposed system must satisfy the following access management requirements:

- **Unambiguous.** Access must be granted through clear and affirmative action to prevent any ambiguity.
- **Informed.** The data owner must provide comprehensive information regarding the use of their data.
- **Freely given.** Individuals must freely and voluntarily give their consent. It is necessary that data owners remain informed of all potential consequences of their access.
- **Specific.** Requests for access must have an explicit objective and be specific. As a result, the person whose data is being processed must be notified of why and how their data is used.
- **Auditable.** The recording of all access data is required to facilitate further audits and to provide legal evidence if necessary.
- **Withdrawable.** The data owner must have the ability to revoke or withdraw previously granted access.
- **Explicit.** Access requests should be clear and informative, specifying the purpose of the request and the data being requested.

4.3 Transparency

Transparency is a fundamental requirement for any system designed to ensure lawful actions and prevent non declared activities that could compromise patient privacy. It is imperative that patients are informed about all actions related to the access of their data once they have granted permission to healthcare providers (Ri). To ensure transparency, the system permanently records every activity, making it accessible at any time.

5 System Architecture

The current section presents our proposed patient-centric access mechanism, as well as the design and architecture of the system, all possible actions related to access management, and proposed algorithms that enable the decision-making mechanism. In this system, three types of participants are considered: Regulatory Authority (RA), Data Requestor (Ri), and Patient (Ui). Furthermore, Fig. 2 illustrates an ideal scenario of the system where we assume that all participants are authenticated. From Steps 1.1 to 1.3, Ri requests access to data through SC1. SC1 checks Ri's legitimacy to access

the system. Once legitimacy is checked, SC3 sends an access request to Ui through the blockchain network with sufficient information about the data requestor and usage. In Step 2, SC2 is triggered to transfer measured data to decentralized storage such as IPFS. From Steps 3.1 to 3.3, Ui grants access to data with a limited time t for usage. From Steps 4.1 to 4.5, the Data requestor accesses patient data. SC4 checks access validity and sends all access activities to Ui. SC4 triggers SC3 to change access status from granted to revoked once t expires. In Step 5, RA bans a Data requestor. Moreover, we define the local views λ (send and receive actions) of every participant which will use them later for security proof.

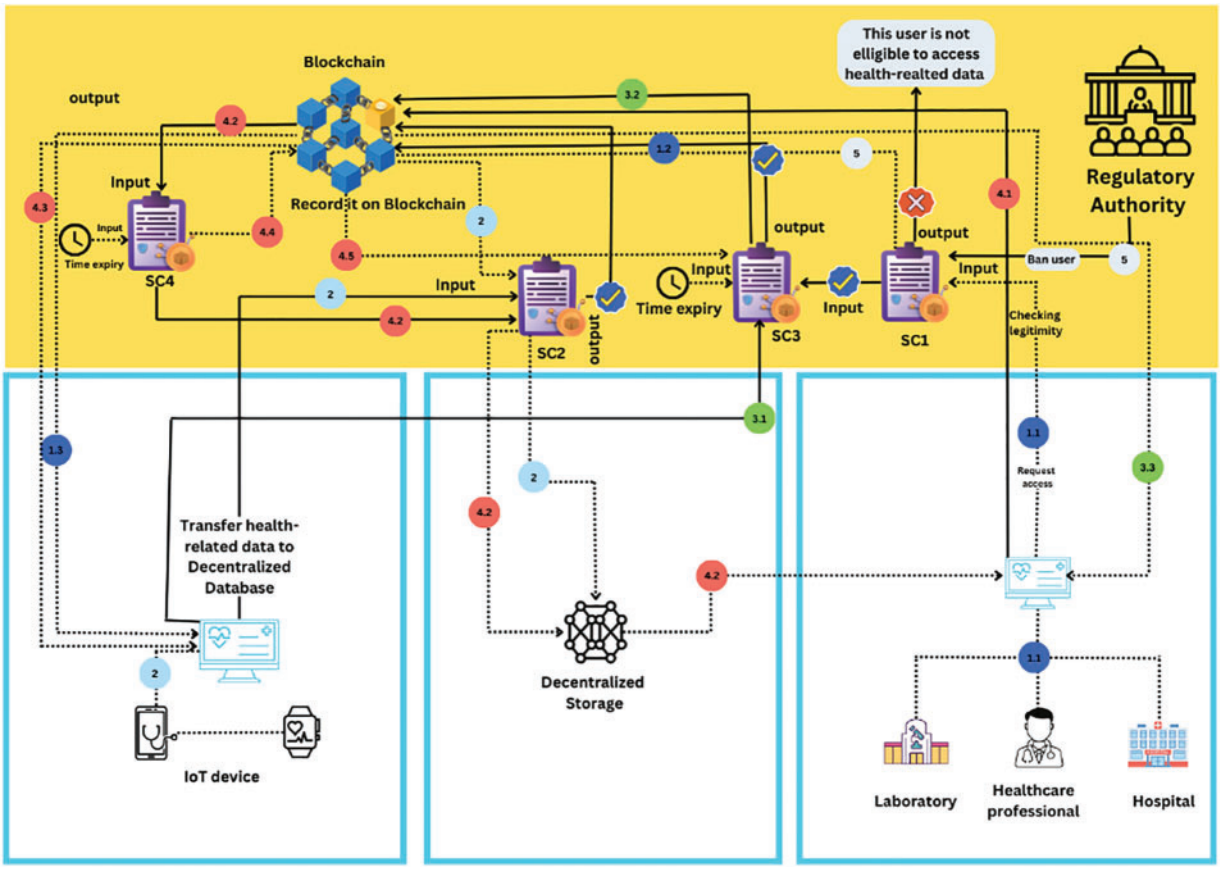

Figure 2: System architecture

- **Regulatory Authority (RA).** RA could be a public healthcare organization (Healthcare Ministry) that has a neutral position and acts in the public interest. In our system, RA is responsible for checking the user's identity and providing a node that performs authenticated actions in the system. The system incorporates multiple security layers, with RA serving as the initial layer. Further, unauthorized nodes are not eligible to request access or perform transactions. Hence, they could not attack the network or attack smart contracts. RA has two sending actions: add authorized nodes or ban existing nodes, and one receiving action from Ui that reclaims unlawful access from Ri.
- **Data Requestor (Ri).** This stands for the healthcare provider, which could be a hospital, a doctor, etc. Ri can request access to the patient's data Di. In our system, Ri has one sending action:

access request to access patient's data Di (Note: Ri is able to access stored data or request measuring new data by means of wearable devices). In addition, Ri has two receiving actions: the decision made by the patient to access data Di (grant/Revoke) and notification related to withdrawn access ReFi (A unique number that refers to access).

- **Patient (Ui).** Patient is the data owner who can control and manage access to their data Di (Access manager). In our system, the patient has two sending actions: grant/Revoke access request to access data and revoke/withdraw a current access ReFi. Additionally, Ui has one receiving action access request made by Ri. Table 2 summarizes the actions of every participant in the send and receive.

Note: These actions will be recorded in an immutable ledger (Blockchain) to ensure trust among users (Transparency and accountability).

Table 2: Local view summary

Participants	Send actions	Receive actions
Patient (Ui)	Grant/Revoke access request; Withdraw a current access ReFi.	Access request made by Ri.
Data Requestor (Ri)	Access request to access patient's data Di.	Patient's decision; Withdrawn access to ReFi.
Regulatory Authority (RA)	Add authorized nodes; Ban existing nodes.	Ui claims unlawful access from Ri.

5.1 Formalizing the Possible Actions

The blockchain built-in features record all performed actions A1, . . . , An in an immutable ledger and make them viewable and auditable to all authentic users P. Therefore, this feature makes the system more reliable and transparent to all acting users. Moreover, the users will be more informed about what happens in the system based on their own local. In addition, Table 3 summarizes all the possible access-related actions A1, . . . , An. Hence, all these actions can be formalized as it consists of three main parts: Action, Entity (Ui, Ri), and Parameters.

Table 3: Possible access-related actions

Actions (Ai)	Meaning
Access request (SendAccessRequest, R_i, (AccessToAccess/AccessToMeasure, ReFi))	R_i Sends access requests to access patients' data or measure new data.
(ReceivedDecision, U_i, (R_i, AccessToAccess/AccessToMeasure, ReFi))	On the other hand, U_i receives the access request and makes the access decision.
Access response	U_i Sends access response to R_i.

(Continued)

Table 3 (continued)

Actions (Ai)	Meaning
(SendAccessResponse, U_i, (AccessDecision ReFi))	On the other hand, R_i receives access response and processes the access decision made by U_i.
(ReceivedResponse, R_i, (U_i, AccessDecision, ReFi$_i$))	
Access-Report (SendDataAccessReport, R_i, (AccessActivitiesUpdates, ReFi)) (ReceiveDataAccessReport, U_i, (R_i, AccessActivitiesUpdates, ReFi$_i$))	Once R_i is granted access to the patient's data, BC/R_i sends all activities related to access Ref_i to U_i.
Withdraw access (SendRevokeAccess, R_i, U_i, (RevokeAccess, ReFi)) (ReceivedRevokeAccess, R_i, (U_i, RevokeAccess, ReFi))	Once U_i sends a revoke/withdraw decision of access with ReFi. Then, R_i gets notified of the access withdrawal decision made by U_i.

5.2 Smart Contract Design for System Functioning

This section covers the suggested smart contract SCi, which initially consists of verifying the data requestor's authenticity and the legitimacy of the accessing activities. Additionally, it is for the purpose of automatically switching access status based on a withdrawal decision made by the patient or expiration of the defined period of time t. Furthermore, it is used to transfer measured data Di to decentralized storage. The system design includes the following four smart contracts to accomplish this objective:

- **Smart Contract 1 (SC1).** It first verifies the identity of users, particularly healthcare providers (Ri). Additionally, the Regulatory Authority (e.g., the Healthcare Ministry) acts as the smart contract owner. The RA has the ability to add new users or ban existing ones. The output is recorded in the Blockchain to identify the trusted and banned users. Therefore, based on the SC1 property that provides trustworthiness and authenticity to users, the design goal can be formalized as follows:

Design Goal 1. *It is authentic for Ui that actions Ai...An are performed by authentic and trustful users (Authentication).*

- **Smart Contract 2 (SC2).** It takes the data hash, the date and time of data measurement, and other relevant details as input parameters. The output is stored in the Blockchain. Then, the measured data is stored off-chain. As a result, the data's authenticity is verified through blockchain. Therefore, the design goal can be formalized as follows:

Design Goal 2. *It is authentic for Ui that the measured data by the wearable health-based devices remain the same when transferred to the decentralized storage (Data integrity).*

Design Goal 3. *It must be authentic for Ri that the received data is the data that Ui transferred to the decentralized storage and was measured using Ui's health-based devices (Data authenticity).*

- **Smart Contract 3 (SC3).** It allows healthcare providers to request permission to access data. Additionally, it enables patients Ui to grant access by setting a time limit *t* or to revoke/withdraw current access to ReFi. The smart contract SC3 can automatically revoke access once the

specified period t has expired. Therefore, access will be unlawful. Once the healthcare provider requests access, SC3 triggers SC1 to ensure that Ri is not a banned user, and then Ui receives the request. The output is stored in the Blockchain. Therefore, the design goal is as follows.

Design Goal 4. *Each granted access is authentic for all users ∈ P, and remains valid until t is expired or Ui revokes access ReFi (Access authenticity).*

- **Smart Contract (SC4).** It checks the validity of accessing Di by Ri based on access ReFi. It enables the system to detect unlawful access. SC4 is triggered, once Ri initiates an action Ai to access data. SC4 takes SC1's output as an input, and the access ReFi.

Design Goal 5. *It must be authentic for Ui that Ri can access data uniquely based upon the access ReFi (Data confidentiality).*

Note: Ri is authenticated by the Regulatory Authority (RA), once joining the system. Hence, Ri can perform transactions by sending access request through blockchain account to user Ui (Patient) who is the owner of data Di. Further, Ui receives access request and sends back access decision (Grant/Revoke) to data requestor Ri via blockchain account.

5.3 System Process

The sequence diagram provided in Fig. 3 highlights the step-by-step access request process. In addition, before Ri performs any transaction, SC1 is automatically executed to report if Ri is a trusted or banned user. If Ri is banned, action Ai becomes invalid. On the other hand, if Ri is a trusted user, action Ai becomes valid, and Ri is allowed to request access such as follows:

- **Step 1.1:** Healthcare provider Ri performs and signs a transaction (Ai action or a set of actions A1 . . . An) through blockchain account to request access to Ui's data Di or start measuring new data Di. The transaction contains many input parameters, such as Pi purpose to access Di, data type, Ni nature (Old or new data Di), and time t required to access data.
- **Step 1.2:** After the transaction is being signed by Ri, it will be propagated through the network for validation. Then, it is recorded on the Blockchain within a new block after reaching consensus among nodes.
- **Step 1.3:** The patient Ui checks the access request after it is received and verified by their Ui blockchain account.
- **Step 2:** Ui decides whether to grant or Revoke the request based on inputs delivered by Ri.
- **Steps 3.1 and 3.2:** The decision made by Ui is sent to Ri for notification, and stored within a block in the ledger (If Ui grants access, a reference number ReFi is automatically generated in order to be used by Ri as input in SC4.)
- **Step 3.3:** Ri receives the decision through a transaction Ai performed by Ui via blockchain network. The Ri's blockchain account receives and verifies it in order to be presented to Ri.

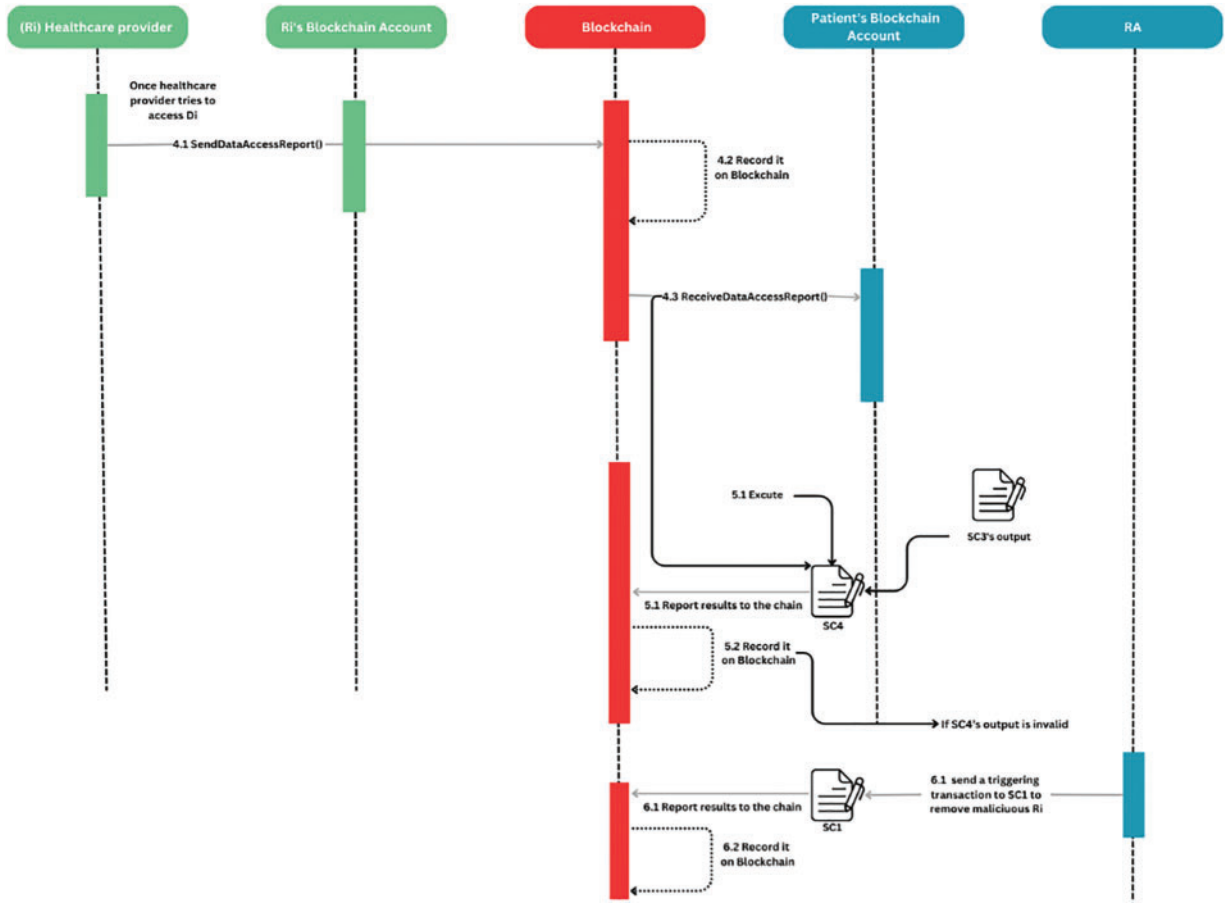

Figure 3: Step-by-step access process

Furthermore, following to Step 3.3, Fig. 4 illustrates the process by which the validity of accessing data is checked according to patient Ui's decision (Grant/Revoke). SC4 ensures the enrolment of this process. As a result, it satisfies DG5.

- **Step 4.1:** Once Ri receives the Ui's decision with valid access ReFi, Ri can access measured data Di or measure new data using Ui's devices for a predefined period of time t. Furthermore, Ui is informed of all access activities, with sufficient details of what actions performed by Ri.

Note: Ri can only access newly measured data Di until it is stored in the decentralized storage database.

- **Steps 4.2 and 4.3:** Once Ri performs a transaction, Ai through the network in order to access Di. Ui receives an access report to their blockchain account.
- **Steps 5.1 and 5.2:** At this stage, SC4 is automatically executed to check access validity or inappropriate behavior by Ri. SC4 output is recorded in the chain. To this end, SC4 ensures that DG4 is held in the system.
- **Steps 6.1 and 6.2:** If SC4 's output is invalid, RA initiates a transaction Ai to execute SC1 to ban Ri from the system. SC1 output is recorded in the chain. To this end, SC1 ensures that DG1 & DG5 are held in the system.

In addition, according to GDPR, Patient Ui is able to revoke/withdraw granted access ReFi at any time. Then, Ri will automatically get notified of the patient's new decision following the steps below:

- **Step 1.1 Revoke:** Ui revokes the granted access ReFi to Ri.
- **Step 1.2 Revoke and 1.3 Revoke:** Ui initiates a withdrawal transaction Ai and sends it back to Ri via the blockchain account.
- **Steps 1.4 Revoke:** Ri gets notified of the decision to revoke the access via blockchain account after being received and verified.
- **Steps 2.1 Revoke and 2.2 Revoke:** At this stage, SC3 is automatically executed if t is expired. SC3 changes access status to invalid. Hence, these steps enable DG4 to be held in the system.
- **Step 2.3 Revoke:** The new access status is recorded within a block in the ledger for a later audit trail.

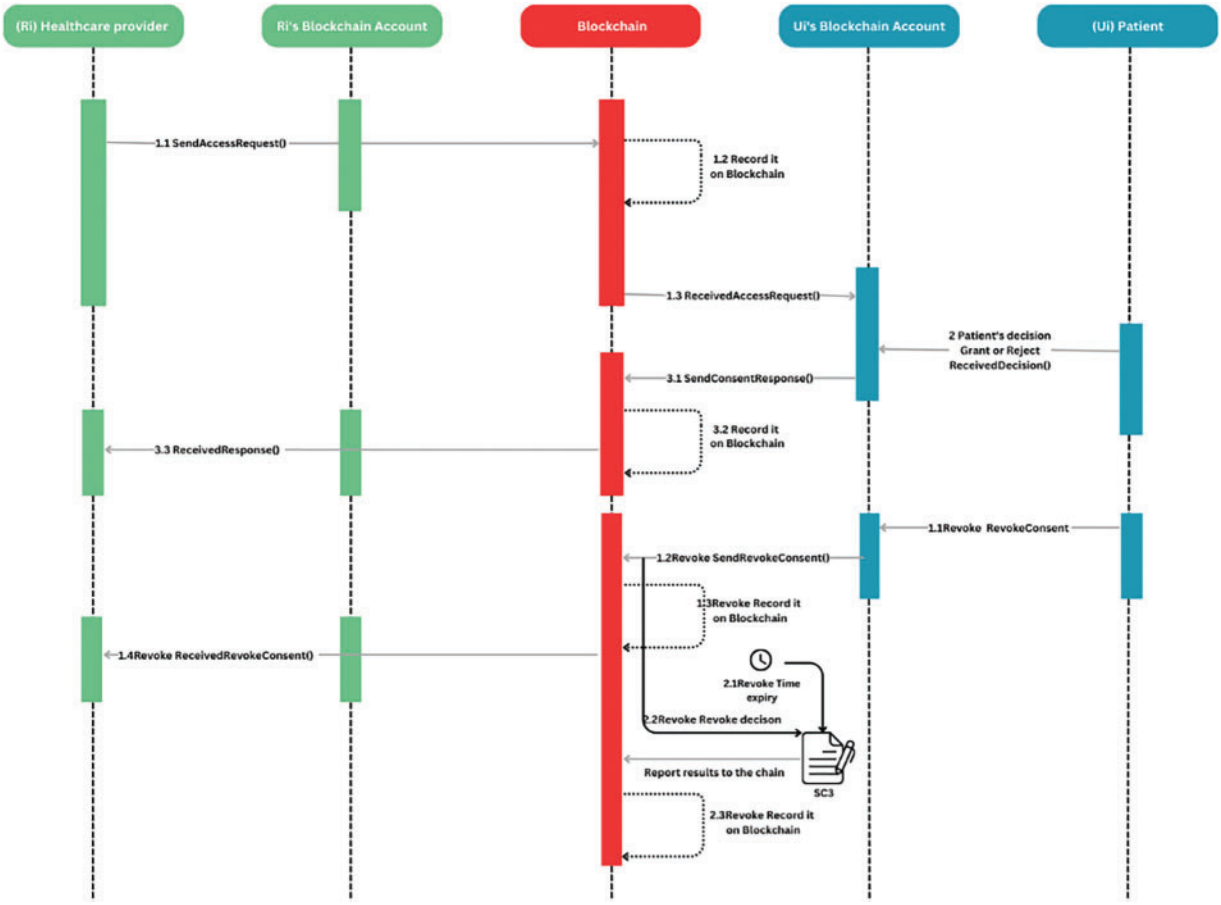

Figure 4: Access activity process

5.4 The System Trustworthiness

This section discusses the trustworthiness of the system through the trust assumptions made based on blockchain technology properties, which can be utilized for the formalization and validation of the system's security properties by applying the security modeling framework SeMF. Further, the term trustworthiness expresses the degree to which a particular trust assumption is achieved through the

system properties [26]. As discussed earlier, the system design includes three main users P: Ui, Ri, and RA, with a unique local view λ by which users interact with the system. Further, the patient is the data Di owner and can share their health-related data with only trusted users Ri. For example, the patient has full trust in the system's properties, their data Di cannot be shared with unreliable users, and the patient is able to revoke access at any time. Hence, the system's trustworthiness proves the authenticity of all access-related actions that are performed by an authentic user, and all access-related data is permanently stored. To this end, the built-in blockchain features can contribute effectively to ensure our system's trustworthiness. These features include authenticity, integrity, availability, nonrepudiation, ledger immutability, auditability, etc. Therefore, Blockchain provides an immutable and transparent record of all access-related transactions that occur. Hence, it ensures trust in results shown to the users even after a series of actions ω.

However, in a public blockchain, all data and transactions that are recorded within blocks can be visible to all nodes in the network, which presents some privacy issues. As a result, health-related data or any sensitive data cannot be recorded in the ledger. This issue was addressed in the proposed system, to store all health-related data or other sensitive data in a decentralized storage database such as IPFS [11] in an encrypted form with the use of encryption methods such as the homomorphic encryption approach [30] or Advanced Encryption Standard same as implemented in [31]. Furthermore, other ways of storage can be explored such as introduced in [32] Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control. That relies on a server cloud with the use of a proxy re-encryption scheme to enhance data security. In our system, only access-related transactions are stored in the ledger. Further, to strengthen the security of the system, RA, by means of SC1, works as the first security layer to add only trusted nodes and ban untrusted ones.

Moreover, the key characteristics of Blockchain especially those based on cryptography can contribute positively to enhance the system's security and ensure privacy. The trust assumptions relaying on Blockchain's security properties.

Trust assumption 1. *All received actions A1 . . . An from Blockchain are whether previously performed and signed by authentic users P or by triggered SCi once a set of conditions are met (Authenticity/Digital signature/Smart contract).*

Trust assumption 2. *All added actions A1 . . . An to the chain must be authentic (Authenticity).*

Trust assumption 3. *Any measured data by the wearable health-based devices remains the same when transferred to the decentralized storage. It is achieved by the mean of hash value stored in the Blockchain (Data Integrity).*

Trust assumption 4. *Any transaction-related data shown on the user's blockchain account must be previously transferred to Blockchain and signed by an authentic user or a smart contract (Authenticity/Digital signature).*

Trust assumption 5. *Once a user ∈ P performs a transaction and sends it through the network, the transaction-related data remains unchangeable once added to the chain within a new block (Authenticity/Integrity).*

Trust assumption 6. *SCi can be automatically executed once certain conditions are met (Automation/Smart contract).*

Trust assumption 7. *All performed A1 . . . An are timestamped and permanently added to a chain within a block following a certain order. The block is validated and linked to the last block in the chain by the mean of a consensus algorithm (Timestamp/Order proof).*

Trust assumption 8. *Every node in the network keeps a copy of the whole ledger (Distribution/Immutability/Proof of evidence).*

6 The Security Properties & GDPR Compliance

As stated previously in Section 5, the security modelling framework SeMF [27] is primarily targeting the modelling and validating the security properties. This framework uses formal languages and is independent of specific representations of the system [27]. Further, SeMF has introduced a variety of formal definitions regarding the security properties among others Authentication and Proof of authenticity. Those definitions are used alongside this section to formally prove that the defined design goals are held.

6.1 Authentication

The purpose of authentication is to verify users' identities within the system and to guarantee that actions A1, ..., An are authentic. The authentication property is formalized and validated using the following two definitions:

1-A set of actions $\Gamma \subseteq \sum$ is authentic for $P \in \mathbb{P}$ after a sequence of actions $\omega \in B$ with respect to WP if $alph(x) \cap \Gamma = \emptyset$ for all $x \in \lambda - 1$ P $(\lambda P(\omega)) \cap WP$.

2-For a system S with behaviour $B \subseteq \sum *$, user $P \subseteq \mathbb{P}$, and actions a, b $\in$ 6, auth(a, b, P) holds in B if for all $\omega \in B$, whenever $b \in alph(\omega)$, the action a is authentic for P.

6.1.1 Formalization

The defined smart contract SC1 works as the first security layer of the system, which helps the Regulatory Authority RA to establish an identity verification before adding new users to the system. By doing so, any blockchain type, public or private, can be implemented in the system. Further, in our proposed system, all users $\in$ P are verified by RA. Hence, every user $\in$ P and SCi has a blockchain account, which works as a middle interface between the user and the system. Every user $\in$ P needs to acquire a blockchain account that holds (Ski, Pki) pairs [28]. The account enables the user to perform new transactions and sign them using the secret key Ski. Further, the performed transaction is validated by the blockchain network using the user's public key Pki (Authentication verification). Then, the transaction is added to the Blockchain within a block and linked to the last block once consensus is reached (Trust assumptions 7 and 8).

6.1.2 Validation of Authentication

As stated above, every user $\in$ P has a blockchain account, which enables the user to perform the validation process of the digital signature. As a result, the user's blockchain account validates the authenticity. Further, the blockchain network checks the origin of the transaction and adds only digitally signed transactions with the user's secret key Ski (Trust assumption 4). Further, every user in the system can hold only one blockchain account. Users can claim ownership of an account through Ski. Further, every blockchain account has an address created using Pki, which is used to identify the users P in the system [28]. Further, once Ri performs an action Ai, it is necessary to be signed only with Ri's secret key (It needs to be kept secret and not shared with anyone). Then, it will be verified by SCi's blockchain account using Ri's public key and presented to the patient. Hence, from the blockchain perspective, it is necessary to ensure that the performed action Ai is authentic and originated from an authentic user.

The proposed system's design goals DG1 and DG4 are ensured by built-in features of the Blockchain, among others, the digital signature (**Trust assumptions 1 and 4**). Further, the same applies to DG1 and DG 3, where the authenticity of all sets of action trust is assumed (**Trust assumptions 2, 5, and 7**).

6.1.3 Authentic Actions

As stated above, every user ∈ P has a local view λ. Further, the user can check only his own sent and received actions A1 . . . An. Hence, their authenticity is equivalent to **Auth(Send, Receive, user).** Stated otherwise, if an action occurs in a sequence of actions ω, then the user can legitimately claim that action Send occurred before action Receive. Therefore, the authenticity of the aforementioned actions is verified using Definitions 1 and 2 of the SeMF.

Note: user1 is denoted as the sender, while user2 is the receiver.

Proposition 1. *User1's matching sent action Send is authentic if user2 executes the received action Receive*.

Proof of Proposition 1. The authenticity of the actions can be verified using the trust assumptions 1, 2, 5, and 7. In this part, only one received action example is used for proof of concept, as the same can be applied to the rest of the actions. Moreover, whenever user1 (Ri) sends access request action Send, the user1 authenticity is verified to user2 (Ui) via SC1 before Ui performs the received action Receive (ReceivedDecision, Ui, (Ri, AccessToAccess/AccessToMeasure, ReFi)). As a result, the authentic send action Send for Ui is (SendAccessRequest, Ri, (AccessToAccess/AccessToMeasure, ReFi)), which is denoted as a set of actions Γ in this case. In other words, it must be authentic for all series of actions ω that include action Receive. As a result, Proposition 1 can be validated as follows:

- Once user2 receives action Receive then the matching action Send performed by user1 was already recorded in the Blockchain (**Trust assumptions 1 and 7**).
- When user1 adds the action Send, then it is authentic (**Trust assumption 2**).
- When an action is authentic, the data that is transmitted and received are identical (**Trust assumption 5**).

Moreover, DG3 is achieved. Below is how to formalize this:

Auth(SendAccessRequest(AccessToAccess/AccessToMeasure, ReFi), ReceivedDecision(Access ToAccess/AccessToMeasure, ReFi), Ui)

Note: Proof 1 can apply to all potential sent and received actions in the system.

Moreover, trust assumptions 6, 7, and 8 can guarantee that DG1, DG4, and DG5 hold in the system. They allow all performed actions in the system to be recorded on a distributed ledger in the form of linked blocks. Hence, the trust assumptions provide secure and reliable data storage and make all actions transparent and auditable to all users ∈ P. As a result, every user ∈ P can have an expandable knowledge of the system's actions denoted as ε beyond the user's local view λ. Moreover, according to trust assumption 6, the smart contract's characteristics of reliability and inevitability proved that DG1, DG4, and DG5 are held in the system.

Proposition 2. *The action Send associated with the smart contract is authentic if user B executes the action Receive*.

Proof of Proposition 2. Proposition 2 is validated the same way as Proposition 1 was validated. Hence, the trust assumptions 1, 3, 5, 6, and 7 are best describing user2's initial knowledge W2.

- When user2 performs action Receive, the corresponding action Send is recorded in the distributed ledger which is sent by smart contract in form of a transaction (**Trust assumptions 1 and 7**).
- When smart contract adds the action Send, then it is authentic (**Trust assumptions 3 and 6**).
- When an action is authentic, the data that is transmitted and received are identical (**Trust assumption 5**).

To this end, since DG4 and DG5 are held in the system, SC3 and SC4 are used.

6.2 Proof of Authenticity

To formalize and validate the proof of authenticity in order to prove the system's authorization, nonrepudiation, and integrity properties. The SeMF's Definition 3 is used as follows:

Definition 3 (Proof of authenticity). For a system S with behavior $B \subseteq \Sigma*$ and actions $a, b \in \Sigma$, precede(a, b) holds in S if for all $\omega \in B$ with $b \in \text{alph}(\omega)$, it follows that $a \in \text{alph}(\omega)$.

Proposition 3. *If user2 performs the action Receive, user2 must have access to proof in order to show other users that the matching sent action Send occurred prior to the received action Receive*.

Blockchain functions as a proof of evidence, by ensuring that all associated data and transactions are permanently recorded in a distributed ledger. Due to its design, Blockchain is immutable and cannot be altered without affecting all subsequent blocks in the network. It offers also timestamped records. These inherent features of Blockchain, such as immutability and nonrepudiation, enable us to leverage assumptions 7 and 8 for proof of authenticity.

Proof of Proposition 3. Proposition 3 is validated the same way as Proposition 1 was validated. Hence, the aforementioned assumptions 7 and 8 are best describing user2's initial knowledge W2.

- User2 can retrieve the recorded transaction-related data associated with the action Receive after receiving the action (**Trust assumption 8**).
- Once user2 can access the recorded transaction-related data associated with the action Receive then user2 can prove the action Send has occurred before the action Receive (**Trust assumption 7**).

Consequently, the properties of nonrepudiation, integrity, and authority are proven by formalizing and verifying the proof of authenticity.

6.3 Implementation

In our implementation, we used the Ethereum development tool Remix IDE. Additionally, smart contracts code is written in the Ethereum programming language Solidity. The smart contracts code has passed the security analysis with the help of Remix IDE built-in security tool and Mythril tool. In our testing case, we consider that all system participants have their own Ethereum addresses, and the smart contracts are deployed and owned by the Regularity Authority. The performance was tested on the Sepolia testnet, which has an average transaction time of 13 s. The following table summarizes the gas consumption of each function call. Thus, the experimental results have demonstrated the efficiency of the system in terms of time and cost savings, as shown in Table 4.

Table 4: Gas consumption analysis

Function	Gas consumption
SC1: Add_user()	123,005
SC1: Ban_user()	40,568
SC2: Add_file()	141,456
SC3: Send_access_request()	131,890
SC3: Send_access_decision()	119,012
SC3: Revoke_access()	59,836
SC4: Check_access_validity()	70,698
SC4: Send_access_activity()	83,461

6.4 GDPR Compliance

Having established the necessity of employing SC3 and SC4 based on the formal definition of SeMF, including authentication, the following section delves into the compliance of our proposed solution with the General Data Protection Regulation (GDPR) as outlined in Section 5. By using SC3 and SC4, we ensure that our system meets the standards of the GDPR. This compliance is crucial for establishing trust and confidence among users.

In the following subsections, we will explore in detail how our system adheres to GDPR regulations of data protection and privacy:

- **Unambiguous:** By eliminating any ambiguity regarding the period of access SC3 guarantees that access is granted for a specified duration t. This precise time-bound access control is crucial for maintaining data security and user trust.
- **Informed:** By using SC3, it guarantees to the patient a comprehensive information regarding the purpose for which their data is being utilized and the identity of the individual or entity requesting access. This transparency empowers patients to make well-informed decisions about their personal data.
- **Freely given:** In order to guarantee that access is granted voluntarily and without any kind of force, the patient has the entirety of right for denying the request. This aspect is guaranteed by SC3.
- **Specific:** The use of SC3 allows the patient to be informed about the specific nature of the data being requested and the precise purpose for which it is needed. Additionally, SC4 facilitates the patient's awareness of when their data is accessed and by whom, thereby enhancing accountability and trust.
- **Auditable:** The Blockchain is used to systematically record all transactions, making it possible to retrieve them at any given moment for the purpose of eventual verification. This feature guarantees complete traceability and transparency, which are crucial for regulatory compliance and building trust among stakeholders. The immutable nature of blockchain technology provides an indelible record of all activities, facilitating audits and investigations with ease and precision. This capability not only enhances accountability but also supports the integrity of the data management process, ensuring that all actions can be traced back to their origin.
- **Withdrawable:** The implementation of SC3 empowers patients with the ability to withdraw or revoke access to their data at any time. This mechanism also guarantees valid access for

the predetermined period (t), thereby offering flexibility and control over personal data. Such a feature is vital for adapting to changing circumstances and maintaining the autonomy of patients over their own data. It also underscores the importance of dynamic consent management, by allowing patients to modify their consent preferences as needed, SC3 supports a responsive and patient-centric approach to data privacy.

- **Explicit:** SC3 guarantees that patients are explicitly informed about the data being requested, thereby eliminating any potential for confusion or misinterpretation. This clarity is essential for fostering informed consent and trust. By providing detailed and clear information about data requests, SC3 helps patients understand the implications of their consent, thereby enhancing their confidence in the system and ensuring that their rights are respected.

6.5 Comparison with Existing Works

Table 5 highlights a comparison of our system with existing solutions. All systems, including ours, support patient-centric access control. In addition, only reference [16] and our system provides authentication. All systems claim to ensure data integrity, but reference [18] notes a risk when patients are involved in the data upload process. Thus, our system ensures data integrity. All systems, including ours, ensure data authenticity. Further, solutions [15–18] have conditional access authenticity, with access granted for an unlimited period and revoked by the patient. Our system grants access for a limited period, with the patient able to revoke access before the period ends. All systems, including ours, ensure data confidentiality. Only reference [16] and our system are GDPR compliant.

Table 5: Comparison with existing solutions

	[15]	[16]	[17]	[18]	Our system
Patient-centric access control	Yes	Yes	Yes	Yes	Yes
DG 1 Authentication	No	Yes	No	No	Yes
DG 2 Data integrity	Yes	Yes	Yes	Yes/No, involving patients in the data upload process poses a risk to data integrity.	Yes
DG 3 Data authenticity	Yes	Yes	Yes	Yes	Yes
DG 4 Access authenticity	Yes/No, access is granted for an unlimited period of time. The access is revoked by the patient	Yes/No	Yes/No	Yes/No	Yes, access is granted for a limited period of time. The patient can revoke access before the period ends

(Continued)

Table 5 (continued)

	[15]	[16]	[17]	[18]	Our system
DG 5 Data confidentiality	Yes	Yes	Yes	Yes	Yes
GDPR compliance	No	Yes	No	No	Yes

7 Conclusion

In this paper, we proposed a blockchain-based access management system designed to enhance patient privacy and secure telehealth and telemedicine data. The solution we propose attempts to be compliant with the General Data Protection Regulation (GDPR) by establishing a patient-centric access mechanism. We detail the design goals and system architecture, outline all potential access-related actions, and present algorithms of the automated decision-making process.

Furthermore, the system design incorporated four smart contracts to ensure our predefined design goals, including data integrity, data authenticity, data confidentiality, access authenticity, and authentication. Smart Contract 1 (SC1) verifies user identities and manages user trustworthiness, ensuring that actions are performed by authentic users. Smart Contract 2 (SC2) verifies the authenticity and integrity of data measured by wearable health devices when transferred to decentralized storage. Smart Contract 3 (SC3) manages data access permissions, allowing patients to grant or revoke access within a specified time limit, ensuring access authenticity. Smart Contract 4 (SC4) checks the validity of data access requests, ensuring that only authorized data requestors can access data based on granted permissions. Thus, these smart contracts provide a robust framework for secure and trustworthy medical data management.

In addition, to ensure the robustness of our system, we formalized and validated its security properties using the Security Modelling Framework (SeMF). This rigorous approach has demonstrated the alignment with the predefined security requirements, including data integrity, data authenticity, data confidentiality, access authenticity, and authentication. Additionally, the system has been compared to other solutions based on design goals and GDPR compliance. As a result, it has proven its efficiency in enhancing patient security and privacy among the existing solutions. Furthermore, the implementation of the smart contracts has demonstrated the cost savings of our system. In the test environment, the average gas consumption ranges between 40,568 and 141,456. Additionally, the high gas consumption of some functions is linked to the additional information in the input.

In conclusion, our blockchain-based access management system not only enhances patient privacy and security but also ensures compliance with GDPR through a patient-centric approach. The combination of decentralized technology and restricted design goals provided a robust and transparent solution for managing patient data, that is mitigating the security and privacy issues of telehealth and telemedicine services.

However, our system demonstrates efficiency in enhancing patient privacy and security, there are several key limitations that need to be addressed in future research:

1. **Scalability:** As the number of users and transactions increases, the Blockchain could be challenged to handle large-scale transactions in terms of latency and computational costs.

2. **Interoperability:** Integrating the Blockchain with existing healthcare systems might be challenging. As a result, to provide data flow between different systems, standardization and compatibility activities are required.
3. **User Adoption:** Promoting widespread adoption of the blockchain architecture among healthcare professionals, patients, and other stakeholders can be challenging. Users may be concerned about the security and privacy of their data.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contributions to the paper as follows: study conception and design: Ayoub Ghani; data collection: Ayoub Ghani; analysis and interpretation of results: Ayoub Ghani; draft manuscript preparation: Ayoub Ghani, Ahmed Zinedine, and Mohammed El Mohajir. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

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

References

[1] A. E. B. Tomaz, J. C. D. Nascimento, A. S. Hafid, and J. N. De Souza, "Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain," *IEEE Access*, vol. 8, pp. 204441–204458, 2020. doi: 10.1109/ACCESS.2020.3036811.

[2] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives," *J. Food Qual.*, 2021. doi: 10.1155/2021/7608296.

[3] C. Chen, S. B. Goyal, and K. Ramaswamy, "BSPPF blockchain-based security and privacy preventing framework for data middle platform in the era of IR 4. 0," *J. Nanomat.*, 2022. doi: 10.1155/2022/2219006.

[4] B. Houtan, A. S. Hafid, and A. D.Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020. doi: 10.1109/ACCESS.2020.2994090.

[5] L. Hutton *et al.*, "Assessing the privacy of mHealth apps for self-tracking: Heuristic evaluation approach," *JMIR Mhealth Uhealth*, vol. 6, no. 10, 2018, Art. no. e9217. doi: 10.2196/mhealth.9217.

[6] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-Based solution," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1746–1761, 2020. doi: 10.1109/TIFS.2019.2948287.

[7] A. M. Saghiri, "Blockchain architecture," *in Applications of Blockchain Technology. Studies in Big Data*. Singapore: Springer, 2020, vol. 60, pp. 161–176. doi: 10.1007/978-981-13-8775-3_8.

[8] E. Zaghloul *et al.*, "Bitcoin and blockchain: Security and privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, 2020. doi: 10.1109/JIOT.2020.3004273.

[9] S. K. Nanda, S. K. Panda, and M. Dash, "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products," *Multimed. Tools Appl. J.*, vol. 82, pp. 32917–32939, 2023. doi: 10.1007/s11042-023-14846-8.

[10] P. Sharma, S. Namasudra, R. Gonzalez Crespo, J. Parra-Fuente, and M. Chandra Trivedi, "EHDHE Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Inf. Sci.*, vol. 629, pp. 703–718, 2023. doi: 10.1016/j.ins.2023.01.148.

[11] A. Bisht, A. K. Das, D. Niyato, and Y. Park, "Efficient personal-health-records sharing in internet of medical things using searchable symmetric encryption, blockchain, and IPFS," *IEEE Open J. Commun. Society*, vol. 4, pp. 2225–2244, 2023. doi: 10.1109/OJCOMS.2023.3316922.
[12] N. Z. Bawany, T. Qamar, H. Tariq, and S. Adnan, "Integrating healthcare services using blockchain-based telehealth framework," *IEEE Access*, vol. 10, pp. 36505–36517, 2022. doi: 10.1109/ACCESS.2022.3161944.
[13] Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Inform.*, vol. 24, no. 8, pp. 2169–2176, 2020. doi: 10.1109/JBHI.2020.2993072.
[14] K. Sheela and C. Priya, "Blockchain-based security & privacy for biomedical and healthcare information exchange systems," *Mater. Today: Proc.*, vol. 81, pp. 641–645, 2023.
[15] R. P. Puneeth and G. Parthasarathy, "Blockchain-based framework for privacy preservation and securing ehr with patient-centric access control," *Acta Inform. Prag.*, vol. 13, no. 1, pp. 1–23, 2024. doi: 10.18267/j.aip.225.
[16] I. Boumezbeur and K. Zarour, "Privacy preservation and access control for sharing electronic health records using blockchain technology," *Acta Inform. Prag.*, vol. 11, no. 1, pp. 105–122, 2022. doi: 10.18267/j.aip.176.
[17] N. U. A. Tahir *et al.*, "Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability," *Technologies*, vol. 12, no. 9, 2024, Art. no. 168. doi: 10.3390/technologies12090168.
[18] D. Shah *et al.*, "Blockchain factors in the design of smart-media for e-healthcare management," *Sensors*, vol. 24, no. 21, 2024, Art. no. 6835. doi: 10.3390/s24216835.
[19] J. Li, X. Luo, and H. Lei, "TrustHealth: Enhancing eHealth security with blockchain and trusted execution environments," *Electronics*, vol. 13, no. 12, 2024, Art. no. 2425. doi: 10.3390/electronics13122425.
[20] X. Mao, C. Li, Y. Zhang, G. Zhang, and C. Xing, "Efficient and secure management of medical data sharing based on blockchain technology," *Appl. Sci.*, vol. 14, no. 15, 2024, Art. no. 6816. doi: 10.3390/app14156816.
[21] S. E. Abed, R. Jaffal, and B. J. Mohd, "A review on blockchain and IoT integration from energy, security and hardware perspectives," *Wirel. Pers. Commun.*, vol. 129, no. 3, pp. 2079–2122, 2023. doi: 10.1007/s11277-023-10226-5.
[22] H. -N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat COVID-19," *IEEE Internet Things Mag.*, vol. 3, pp. 52–57, 2020. doi: 10.1109/IOTM.0001.2000087.
[23] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A block-chain-based framework for security and privacy-assured Internet of Medical Things with effective access control," *IEEE Internet Things J.*, vol. 8, pp. 11717–11731, 2021. doi: 10.1109/JIOT.2021.3058946.
[24] B. A. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment," *Pers. Ubiquitous Comput.*, vol. 28, no. 1, pp. 17–27, 2024. doi: 10.1007/s00779-021-01543-2.
[25] D. K. J. B. Saini, S. Kumar, A. Bhatt, R. Gupta, K. Joshi and D. Siddharth, "Blockchain-based IoT applications, platforms, systems and framework," in *14th Int. Conf. Comput. Commun. Network. Technol. (ICCCNT)*, 2023, pp. 1–6. doi: 10.1109/ICCCNT56998.2023.10306953.
[26] K. Hameed, M. Barika, S. Garg, M. B. Amin, and B. Kang, "A taxonomy study on se-curing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," *J. Ind. Inf. Integr.*, vol. 26, no. 1, 2022, Art. no. 100312. doi: 10.1016/j.jii.2021.100312.
[27] A. Fuchs, S. Gürgens, and C. Rudolph, "A formal notion of trust-enabling reasoning about security properties," in *Trust Manag. IV: 4th IFIP WG 11.11 Int. Conf., IFIPTM 2010*, Morioka, Japan, 2010, pp. 200–215.
[28] S. Liu, R. Zhang, C. Liu, and D. Shi, "P-PBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability," *Comput. Biol. Med.*, vol. 154, no. 3, 2023, Art. no. 106590. doi: 10.1016/j.compbiomed.2023.106590.

[29] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain tech-nology: Architecture, consensus, and future trends," in *2017 IEEE Int. Congr. Big Data*, 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[30] F. N. D. S. Vanin, "A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach," *Sensors*, vol. 23, no. 1, 2022, Art. no. 14. doi: 10.3390/s23010014.

[31] M. Sumathi, S. P. Raja, N. Vijayaraj, and M. Rajkamal, "A decentralized medical net-work for maintaining patient records using blockchain technology," *Cybern. Inform. Technol.*, vol. 22, no. 4, pp. 129–141, 2022.

[32] W. -X. Yuan, B. Yan, W. Li, L. -Y. Hao, and H. -M. Yang, "Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control," *Multimed. Tools Appl.*, vol. 82, no. 11, pp. 16279–16300, 2023. doi: 10.1007/s11042-022-14023-3.