Savitribai Phule Pune University
Army Institute of Technology, Pune
Alandi Rd, Dighi, Pune – 411015.

DEPARTMENT OF COMPUTER ENGINEERING

Onward to Glory

A REPORT

ON

‘A Blockchain-Based Consent Mechanism for Access to Fitness Data in the Healthcare Context”

T.E. (COMPUTER - B)

SUBMITTED BY

Mr. Umang Kumar

UNDER THE GUIDANCE OF

Dr. Sagar Rane

(Academic Year: 2022-2023)

Savitribai Phule Pune University
Army Institute of Technology, Pune
Alandi Rd, Dighi, Pune – 411015.

DEPARTMENT OF COMPUTER ENGINEERING

Onward to Glory

Certificate

This is to certify that the Seminar entitled

“A Blockchain-Based Consent Mechanism for Access to Fitness Data in the Healthcare Context”
has been submitted by
Mr. Umang Kumar (Roll No. 7358)

of TE COMP-B in the Semester - I of academic year 2022-2023 in partial fulfillment of the Third Year of Bachelor degree in ”Computer Engineering” as prescribed by the Savitribai Phule Pune University.

Dr. Sagar Rane
Seminar Guide

Dr. Sunil Dhore
Head of Department

Place: AIT, Pune.

Date: 09/11/2022

ACKNOWLEDGEMENT

I would firstly like to thank the paper authors **May Aljhari**, **Carsten Rudolph** and **Ahmad Salehi Shahraki** for crafting this extremely detail oriented and well structured paper. The research in the original paper is of top notch level.

I am overwhelmed with deference and appreciation to acknowledge my gratitude towards all those who have assisted me in taking these concepts beyond the level of simplicity and developing them into something substantial. The success of this seminar report necessitated a great deal of direction and cooperation from many people, and I am grateful and privileged to have received it from all of the assisting entities.

I owe a debt of gratitude towards **Prof. Sagar Rane**, my seminar guide, for paying close attention to and taking an interest in my work, and for steering me in the proper way throughout my seminar duration by providing all of the required information for establishing a good system. Despite her busy schedule, I am grateful to her for providing me with her fascinating assistance and direction.

I also would like to extend my appreciation towards the Head of the Computer Department **Dr. Sunil Dhore** for his assistance and his constant counsel and leading me in the right direction in the research I performed.

Lastly, I want to express my gratitude to everyone who has assisted me in completing this tiny project, whether directly or indirectly during the making of this seminar report.

Umang Kumar (7358)
T.E. Computer - B

Abstract

The quality of health services is improved by tracking people's health and physical activities with wearable fitness gadgets. There have been more than enough encounters where wearable gadgets such as fitness bands have saved lives of many a people, based on their record of data. These gadgets detect a sizable amount of private information be it pulse rate monitoring, SPO2 monitoring, blood cholesterol levels and much more that is centralized and processed by a third party. Despite the fact that numerous studies have thoroughly examined privacy concerns related to wearable fitness trackers, no study has addressed these concerns by allowing users to govern their data.

Blockchain is a new technology that offers exceptional benefits for addressing privacy concerns in consent management. A blockchain is a type of distributed ledger technology (DLT) that consists of growing list of records, called blocks, that are securely linked together using cryptography. Since there aren't any totally transparent, lawful options for exchanging personal fitness information using data, this study presents an architecture for a decentralised, dynamic, human-centered, and legally compliant consent system based on blockchain and smart contracts. By formalising the security requirements, algorithms and sequence diagrams of the proposed system's operations demonstrate the consent-related data flow among multiple agents. This is then utilised to demonstrate the system's credibility.

For security pattern verification, we apply the techniques for formally proving security properties of systems provided by the Security Modeling Framework SeMF developed by Fraunhofer SIT, following the abstraction levels of the application development process. With SeMF it is possible to validate if properties like trust, authenticity or confidentiality hold under given assumptions. The formal security modelling framework SeMF, which proves the viability of the solution on an abstract level based on formal language theory, the security features of the suggested system were assessed. By leveraging blockchain technology and smart contracts to record user consent, we have demonstrated how blockchain may help fitness providers address privacy concerns.

Contents

List of Figures

Chapter 1

INTRODUCTION

1.1 Overview

People are now exposed to a large amount of their own private health information as a result of the more people recently using wearable fitness technology like smart watches. These wearables monitor a wide range of information, including physiological data and health-related information like blood pressure, steps, and sleep. The use of these technologies for precise diagnosis benefits patients, doctors, and clinical researchers, but there are some privacy issues that have arisen. Subjects have more control over their fitness data because of the General Data Protection Regulation (GDPR), which the European Union (EU) adopted in May 2018 and which requires agreement from data subjects. In an effort to address the privacy concerns identified, the GDPR's permission criteria impose a significant burden for fitness providers to comply.

As a result, many privacy-preserving solutions have been proposed, however they either rely on a single reliable source or are opaque to users, such as those that only allow for a single permission with no right to revoke. Users anticipate that these gadgets will protect their info and uphold their privacy. These issues with the wearable fitness device privacy policy compel us to further increase the level of privacy for the sharing of fitness data depending on user agreement. Therefore, by retaining consent in an unalterable legal archive, our method merges innovations from the fields of legal frameworks, consent management, and advanced fitness data-sharing control.

1.2 Motivation

The author's study tackles privacy concerns in fitness providers' privacy rules by storing all consent from data subjects in immutable storage and providing users with greater information about the recipients of their data. This research's primary objective is to provide a secure system model that enhances data subjects' control over the processing and collation of their personal information while also enabling data controllers and processors to adhere to GDPR requirements.
Transparency: The user is able to see every step of the consent process.
Blockchain can manage joint parties and make sure that all consent-related transactions are legitimate (authenticity) and originate from an indented agent by selecting a

permissioned network, have not been manipulated (integrity) with, and are handled in a (authorization) nonrepudiable manner (proof of authenticity) .
A scalable service, including consent requests and response actions created by numerous agents, can be provided to an expanding number of users and nodes using blockchain-based scalability.
The immutability of records can help with auditing records and decrease instances of disagreement by tracing the history of documents organised in a specific order with timestamps. It serves as a piece of historical proof. Validity checks for consent and the use of fitness data are logically predefined by smart contracts.

1.3 Problem Definition

If the publication were to provide a straightforward explanation of the issue, it could say that the sensitive user psychological data recorded with smart wearables is largely being governed by centralized third party without giving user any actual control over their own data.Many studies have shown an interest in the protection of personal information by fitness tracker companies. Some scholars have called attention to privacy issues brought on by the use of fitness apps. Linguistic analyses by Sunyaev, Mulder, and Hutton have shown a discrepancy between users' comprehension of consent and service providers' subsequent data usage. All of their findings point to the necessity of implementing a little bit more open, people-centric system that makes the aim of data requests crystal obvious. Fitness apps may unintentionally share user data with other organisations, according to a number of studies that examined the privacy risks associated with the behaviour of health and fitness apps.

Despite the fact that certain fitness apps, including Fitbit, Apple's Watch series, and Strava, have switched from the traditional single-time consent to a more adaptable framework for managing user permission, privacy concerns related to their consent procedures still exist. To ensure that their solutions abide by data protection legislation, these three fitness applications use conventional data management systems that exclusively rely on policies. Therefore, technically speaking, a transparency system is not enforced by the present fitness applications. Additionally, these programmes lack a user interface for educating consumers about how third parties can access and share their data..

1.4 Approach

The research technique is covered in this section along with the reasons behind the approaches that were chosen. This study's main objective is to increase user's control over how their fitness related data is processed and promote transparency in data processing to ensure both compliance and privacy. This development is made possible by defining, outlining, and validating the high-level suggested framework for dynamic consent, which includes a rigorous abstract description of the necessary characteristics of smart contracts and blockchain.

To develop and assess our framework for dynamic consent, we used the Design Science Research (DSR) paradigm Peffers suggested. Because utility is the main focus of DSR, it includes finding a highly concerned problem through an iterative way of creating and evaluating solution objects, as opposed to studying an existing artefact. Because no existing solution has been able to satisfy all of our needs, this research uses the DSR approach to address the problem of fitness providers' privacy. As a result, it incorporates an inventive discovery of system artefacts and analyses them using SeMF in a formal abstract description. Using SeMF, which acts as an instrument for demonstrating the reliability of our put forth design model by offering an accurate description of the proposed architecture and its attributes, as well as architecture validation, as Hevner and Peffers stressed the evaluation phase's significance as a "crucial" part of a DSR contribution.

The following is a summary of the proposed system:

- The system must carefully adhere to GDPR's requirements for legitimate permission.
- We shouldn't let the capability of a standard fitness tracker be surpassed by our proposed artefacts.
- To meet the criteria of GDPR compliance and transparency, all system actions must be audited. An automated self-report data access check, a check for data availability, and a robotic change from legitimate to invalid permission based on user decisions were additional features and services required to meet transparency requirements.
- Scalability is a need for the suggested system for keeping and sharing user's consent information between various agents. One of the key specifications used to design system to offer more secured and trustworthy communication is a security solution.

Chapter 2

LITERATURE SURVEY

Survey on Recommended Consent Mechanism

2.1 Transparency

Transparency is the practise of carrying out an agent's tasks in an open manner without any covert actions so that users may observe the flow of their data and have faith in the agent's fairness and honesty. Transparency is essential in every system to achieve privacy and compliance. The APPs and GDPR ensure openness in processing data procedures to increase consumers' trust in the protection of their privacy. Transparency, privacy, and compliance are the three main pillars of transparent systems. Transparency is a must to users regarding the use of their data after they provide their consent to its processing or gathering. To meet this need, the suggested system makes sure that when fitness providers communicate records of data processing with users who have consented to the process, all three key components of a transparent system are taken into account.

2.2 Security

Security is a crucial component of the requirements for the proposed system and consists of a number of security attributes that guarantee the reliability of our system. The fundamental ideas of qualities pertinent to this subject are presented in this part. The proposed system's security criteria are listed in Table 2. We use SeMF to precisely specify the requirements in Section VIII.

A security management platform for business intranets, or SEMF, performs tasks such automating security scanning and managing assets, vulnerabilities, accounts, and knowledge bases. It can be applied to managing internal security.

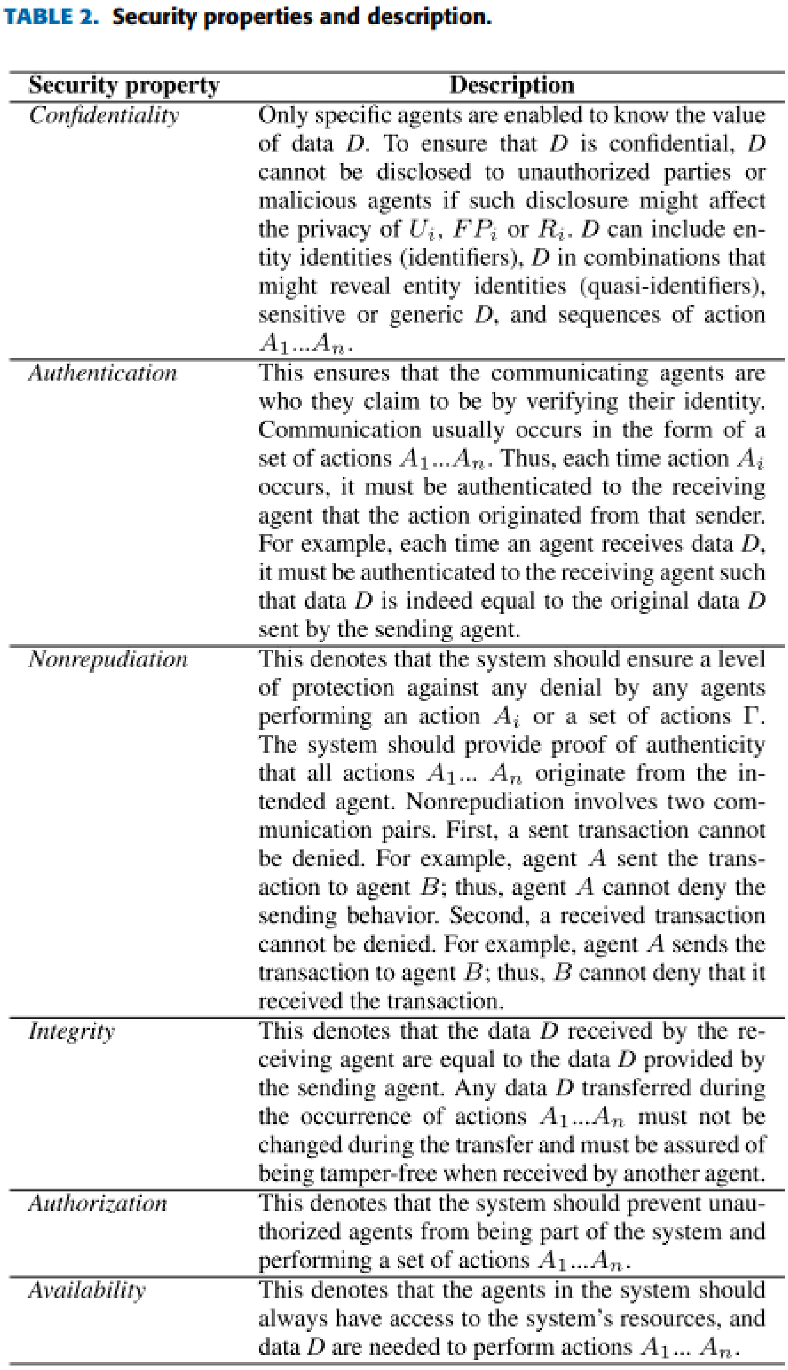


TABLE 2. Security properties and description.

Security property	Description
Confidentiality	Only specific agents are enabled to know the value of data D. To ensure that D is confidential, D cannot be disclosed to unauthorized parties or malicious agents if such disclosure might affect the privacy of U_i, FP_i or R_i. D can include entity identities (identifiers), D in combinations that might reveal entity identities (quasi-identifiers), sensitive or generic D, and sequences of action $A_1 ... A_n$.
Authentication	This ensures that the communicating agents are who they claim to be by verifying their identity. Communication usually occurs in the form of a set of actions $A_1 ... A_n$. Thus, each time action A_i occurs, it must be authenticated to the receiving agent that the action originated from that sender. For example, each time an agent receives data D, it must be authenticated to the receiving agent such that data D is indeed equal to the original data D sent by the sending agent.
Nonrepudiation	This denotes that the system should ensure a level of protection against any denial by any agents performing an action A_i or a set of actions Γ. The system should provide proof of authenticity that all actions $A_1 ... A_n$ originate from the intended agent. Nonrepudiation involves two communication pairs. First, a sent transaction cannot be denied. For example, agent A sent the transaction to agent B; thus, agent A cannot deny the sending behavior. Second, a received transaction cannot be denied. For example, agent A sends the transaction to agent B; thus, B cannot deny that it received the transaction.
Integrity	This denotes that the data D received by the receiving agent are equal to the data D provided by the sending agent. Any data D transferred during the occurrence of actions $A_1 ... A_n$ must not be changed during the transfer and must be assured of being tamper-free when received by another agent.
Authorization	This denotes that the system should prevent unauthorized agents from being part of the system and performing a set of actions $A_1 ... A_n$.
Availability	This denotes that the agents in the system should always have access to the system's resources, and data D are needed to perform actions $A_1 ... A_n$.

Figure 2.1: Security Properties and Description

2.3 Scalability

A scalable infrastructure is necessary since the proposed system heavily relies on improving agreement management among many users. for meeting system requirements, is essential. The quantity of handled per second in terms of consensus nodes, agents, and transactions the three main factors that affect the scalability of a ledger system. As a result, in the system we propose, we blockchain will offer a scalable solution to an increasing number of people of users and nodes, together with requests for and responses to consent actions produced by various agents. nevertheless each whole Despite the fact that node has a copy of the whole blockchain, only the final A greater total is achieved as a result of the chain's recording of accessible transactions and the settlement of self-report data access. throughput.

2.4 Auditability

A built-in characteristic of blockchain technology called auditability maintains all the data in a blockchain unchangeable and impervious to manipulation. The regulatory authority RA can use the consent stored in the blockchain to conduct audits to settle arguments between untrusted actors. Since authenticity and standards for nonrepudiation in security are covered in full in Section VII, this auditability capability can also be utilised to demonstrate compliance with those criteria. Only authorised parties are permitted to validate blocks in the proposed system, which uses a permissioned network. The choice of the consensus algorithm (e.g., PoW, PoS, Byzantine fault tolerance, etc.) will determine how fair the system is to the parties. A 51 % assault on a public blockchain could compromise auditability characteristics, but the proposed approach employs a permissioned network where only authorised participants are permitted to validate blocks.

2.5 Preserve the original functionality of your fitness tracker

This is significant since the original functioning of the system shouldn't be hampered or burdened by the proposed approach because fitness trackers strongly rely on quick processing. Although the GDPR mandates that users must give their approval before their fitness data is handled, obtaining this consent only once at the beginning of the chain is insufficient. To ensure a sufficient level of functionality regardless of the privacy complexity it adds to our suggested system, we create a flexible contract (such as emphContractToProcessDataForTimePeriod()) for a month or year and give users the option to revoke that contract at any time using emphConsentWithdraw(). As a result, the suggested system's privacy criterion is met, and it's processing function won't be too much slower than necessary to discourage people from utilizing it.

2.6 GDPR Compliance

According to the GDPR, consent is legitimate provided it meets the following requirements: it must be explicit, clear, freely given, specified, informed and auditable (as listed below).

- **Unambiguous**. *Pre-selected options are not acceptable as "a clear affirmative action," which is how consent must be expressed.*

- **Informed**. *Before processing personal data, the user/data subject must informed related to such processing.*

- **Freely Offered**. *Freely and without being forced. The data subject/user must be aware of all the implications of their consent.*

- **Specific**. *The request for consent must be specific and have a clear goal. As a result, the data subject must be fully informed of the objectives and procedures involved in data processing.*

- **Auditable**. *All consent data must be kept on file so that it can be audited in the future and used to support legal claims.*

- **Withdrawable**. *Requests for consent should specify how to quickly revoke a permission.*

- **Explicit**. *The consent should contain specific information about the data it pertains to as well as evidence that it was given by the subject of the data. Validation requires that it can be independently verified.*

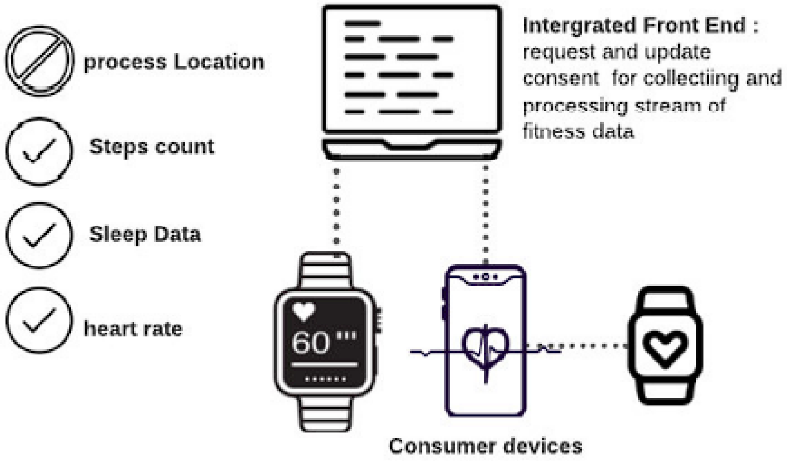


FIGURE 2. Device privacy settings.

Figure 2.2: Device privacy settings

Chapter 3

DEVELOPED SYSTEM

In this section, authors provide their system architectural design model for a blockchain-based authorization system for fitness data access. In terms of the trade, authors suggested solution emphasises privacy and logs all consent procedures in the blockchain. By utilising the built-in security features of the blockchain, this serves as an evidence of permission.

User device privacy settings, recording consent requests and responses and data transmission logs are the system's three main characteristics. These three key components, which track all consent logs and protect against any potentially dangerous activity when the app is running in the background of the phone, ensure that the system complies with the GDPR requirement as stated. As shown in Fig. 2, It is ensured that all data acquisition is done legally based on both user consent and device settings by keeping the user's device privacy settings in the BC. This is one way to prevent such events. Along with the user's level of consent, the device settings serve as an additional layer of privacy protection.

In the proposed system, all consensus-related and sharing data-related operations are documented for auditing purposes on the blockchain, serving as a credible legal archive. When data requesters and fitness providers obtain user permission to analyze or collect their fitness data, this method automatically requires them to do so in the event of a dispute, noncompliance or conflict.

In order to accomplish both privacy and compliance, GDPR promotes transparent data handling. In order to comply with GDPR, the proposed system offers transparency by returning data transaction records to the user. This allows the user to see transparently how their data is transmitted and learn further information regarding the recipients of their data sharing, as well as whether that sharing was done with their consent. With this strategy, all transactions made by the units in the proposed system are transparent to all users of the blockchain network. But, using blockchain to exchange data offers a beneficial solution, it also puts blockchain in opposition to one of the GDPR's requirements, the ”non-remembrance privilege”.

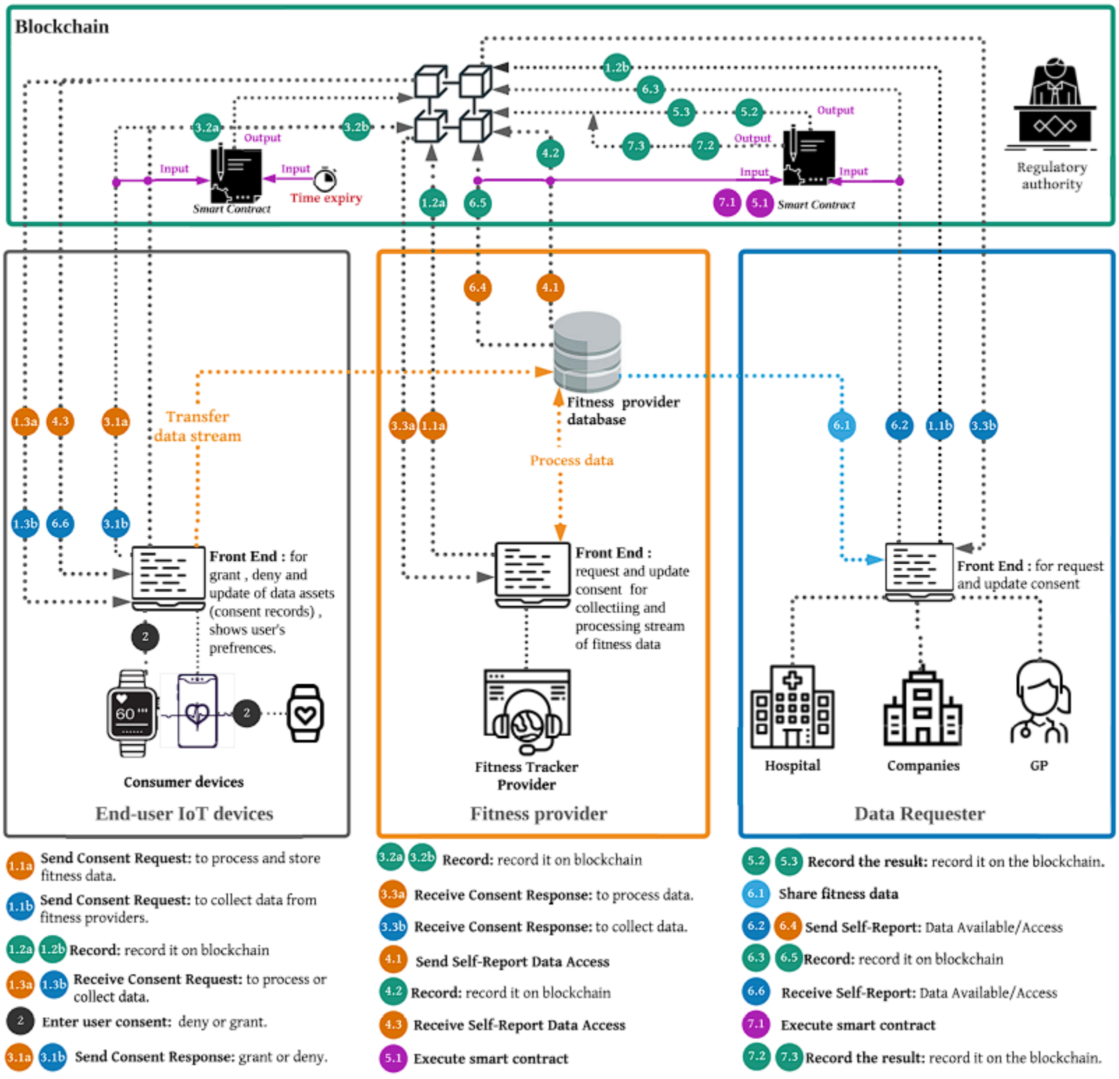

Blockchain
1.2b
6.3
5.3
5.2
Output
3.2a
Output
3.2b
7.3
7.2
Output
4.2
Input
Input
Time expiry
Smart Contract
Input
Input
1.2a
6.5
7.1
5.1
Smart Contract
Regulatory authority
6.4
4.1
Transfer data stream
Fitness provider database
1.3a
4.3
3.1a
3.3a
1.1a
6.1
6.2
1.1b
3.3b
Process data
1.3b
6.6
3.1b
Front End : for grant , deny and update of data assets (consent records) , shows user's prefrences.
Front End : request and update consent for collectiing and processing stream of fitness data
Front End : for request and update consent
2
2
Consumer devices
End-user IoT devices
Fitness Tracker Provider
Fitness provider
Hospital
Companies
GP
Data Requester
1.1a Send Consent Request: to process and store fitness data.
1.1b Send Consent Request: to collect data from fitness providers.
1.2a 1.2b Record: record it on blockchain
1.3a 1.3b Receive Consent Request: to process or collect data.
2 Enter user consent: deny or grant.
3.1a 3.1b Send Consent Response: grant or deny.
3.2a 3.2b Record: record it on blockchain
3.3a Receive Consent Response: to process data.
3.3b Receive Consent Response: to collect data.
4.1 Send Self-Report Data Access
4.2 Record: record it on blockchain
4.3 Receive Self-Report Data Access
5.1 Execute smart contract
5.2 5.3 Record the result: record it on the blockchain.
6.1 Share fitness data
6.2 6.4 Send Self-Report: Data Available/Access
6.3 6.5 Record: record it on blockchain
6.6 Receive Self-Report: Data Available/Access
7.1 Execute smart contract
7.2 7.3 Record the result: record it on the blockchain.

FIGURE 3. Proposed consent management system architecture.

Figure 3.1: Proposed design for a consent management system

3.1 Immutability

Data cannot be deleted thanks to blockchain's immutability feature, which also turns the idea of the "right to be forgotten" on its head. Although the right to privacy is and always will be fundamental one, auditing systems are necessary to make sure that laws are followed. As a result, the suggested system was developed on the premise that consent management and data exchange could be separated. The chain does not store either the data or the pointer to the data. Blockchain does not trade data; instead, it solely controls and records consent- and data-sharing-related operations. Between the person making the request and the person who owns the fitness data, the blockchain functions as an intermediary layer for consent management. Consent requests, consent answers (approval or denial), consent withdrawals, data transmission records, valid report checks of data transmission, and user device privacy environment are all stored on blockchain.

3.2 Requirements Specifications

To be able to understand and explain the algorithms more clearly there is a list of notations and their meaning as used by the authors here.

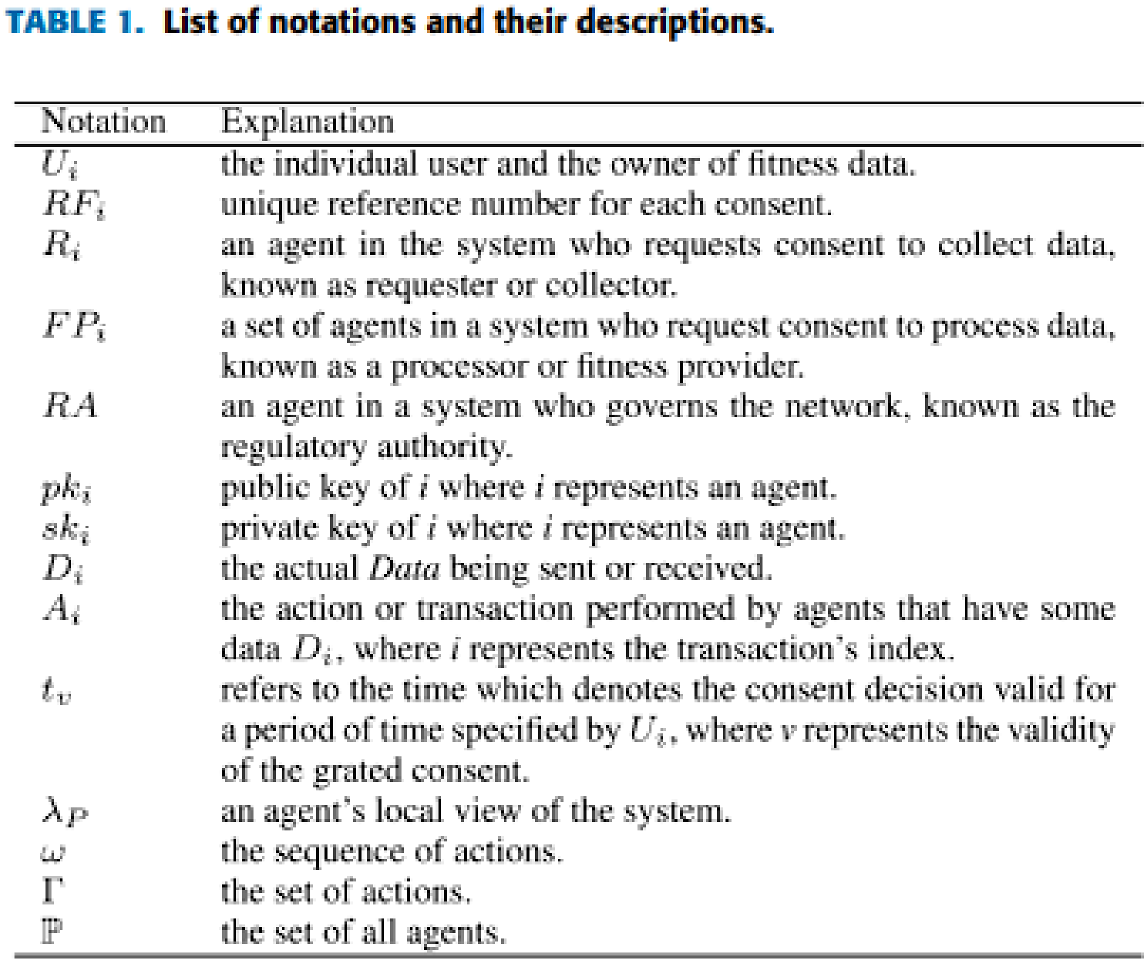


TABLE 1. List of notations and their descriptions.

Notation	Explanation
U_i	the individual user and the owner of fitness data.
RF_i	unique reference number for each consent.
R_i	an agent in the system who requests consent to collect data, known as requester or collector.
FP_i	a set of agents in a system who request consent to process data, known as a processor or fitness provider.
RA	an agent in a system who governs the network, known as the regulatory authority.
pk_i	public key of i where i represents an agent.
sk_i	private key of i where i represents an agent.
D_i	the actual *Data* being sent or received.
A_i	the action or transaction performed by agents that have some data D_i, where i represents the transaction's index.
t_v	refers to the time which denotes the consent decision valid for a period of time specified by U_i, where v represents the validity of the grated consent.
λ_P	an agent's local view of the system.
ω	the sequence of actions.
Γ	the set of actions.
$\mathbb{P}$	the set of all agents.

Figure 3.2: List of notations, together with their descriptions

3.3 System Architecture

This section puts forward the framework for dynamic consent that we designed, together with the system design and architecture, prospective system action sequence diagrams that depict the flow of algorithms and consent-related data that indicate how choices are generated and carried out. We take into account the below mentioned system participants: the user (Ui), the data requester (Ri), the regulatory authority (RAi), and the fitness provider (FPi) . The suggested system is made up of four basic components that each make a particular contribution, as indicated in Fig. 3. Here, we examine their local view, which will be crucial for the security proof.

- **Fitness Provider** *(FPi)*: Send and receive operations represent the local view of FPi. FPi features three sending activities: self-reporting data access, self-reporting data availability, and consent requests to process data. A consent response to the process data is another receiving action that FPi has.

- **Data Requester** *(Ri)*: The send and receive operations are the local view of Ri. Ri has two sending activities: self-report data access and requests for permission to gather data from FPi. Additionally, Ri has one receiving action, which is the acknowledgement that data collection is permitted.

- **User** *(Ui)*: The send and receive operations are the local view of the UI. The three sending activities of Ui: consent responses for data collection and processing and valid consent action withdrawal. Also, there are five receive actions of Ui: two requests for FPi /Ri consent, 3 self-report data accesses, and one data availability action to ensure user transparency. To guarantee trustworthy and secure communication between entities, all of the aforementioned actions are documented in the blockchain.

- **Smart Contract** *(SCi)*: The collecting and processing acts of FPi /Ri are automatically verified as valid by the smart contract SCi. Additionally, based on the expiration period and user's action of withdrawl, it is utilised to automatically change from valid to invalid agreement.

- **Regulatory Authority** *(RA)*: The responsibility of RA is to confirm the legality of the authentication data offered by other companies. The RA in which entities enter their identity identification credentials is used to verify their identities when they first register on the blockchain platform. The suggested system's security is first and foremost ensured by the RA. As a result, untrusted nodes are unable to alter consent, fake transactions, or attack smart contracts.

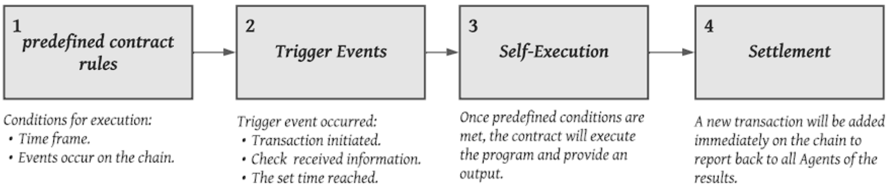

1
predefined contract rules
2
Trigger Events
3
Self-Execution
4
Settlement
Conditions for execution:
• Time frame.
• Events occur on the chain.
Trigger event occurred:
• Transaction initiated.
• Check received information.
• The set time reached.
Once predefined conditions are met, the contract will execute the program and provide an output.
A new transaction will be added immediately on the chain to report back to all Agents of the results.

FIGURE 4. Smart contract execution steps.

Figure 3.3: Smart Contract Execution Stages

3.4 Proposed System Action Sequences and Algorithms

In Table 3 under the headings (Action, Entity, Parameters), the proposed system is made up of a number of consent-related actions 0. In order to formalise the behaviours, the authors develop a mechanism through which fitness providers handle the fitness data that users' wearable fitness devices measure, as well as data processing and sharing by other agents based on users' agreement shown in Fig. 3. Because of this, we employ the procedures shown in Table 3.

Each one of the agents in the system has a local view, designated by the symbol P, in which it can only observe actions it has sent or received. A1. . .An. We can list every agent P's. The design objectives of the suggested system can thus be officially defined as follows. P by identifying the transmit and receive operations carried out by each agent P.

- **DG1:** An agent has to be able to verify that the data displayed on the agent device matches the data sent via the blockchain.
- **DG2:** For agent B, it is legitimate that the data received match those that agent A submitted.

All actions A1.An taken by agent P can be recorded on the chain and seen by all agents P thanks to the blockchain feature. Agent P may be able to enhance their knowledge of system actions beyond transmitting and receiving by way of this method. Table 3 contains a list of all system activities A1...An. We think that they can be accomplished through smart contracts based on the aforementioned presumptions and our understanding of blockchain processes like smart contracts and immutability.

3.5 Overview of the Proposed Method

An illustration of the smart contract SCi execution phases is shown in Fig. 4. We have two automated procedures in the suggested system that we can use to test our smart contract hypotheses. The following are these automated procedures.

- **Smart contract SC1:** If consent was granted, the decision is still valid for a certain amount of time unless it has been revoked. With Ui's permission, we can bound time using a smart contract. The given consent is become void once the allotted period has passed (as shown in Fig. 5). As a result, it would be illegal for FPi or Ri to process or gather data after that predetermined window of time. The sensible agreement The time expiry of SC1 tv and the withdrawal transactions initiated by Ui serve as its input parameters. A very new transaction is added to the blockchain as a result of SC1's output to reflect the consent associated with reference number RFi becoming void. Below, we outline design objectives based on SC1 characteristics that provide agents authenticity, which are loosely defined as follows:
  - **DG3** All agents must be able to verify the granted consent's authenticity in order for it to be valid after the consent time period and Ui's withdrawal choice.
- **Smart contract SC2:** Verify the accuracy of the data collection, processing, and storage based on Ui's given/refused consent With the use of a smart contract, we can identify any misconduct. either FPi or Ri in storing, processing, and collaborating Data on UI's fitness (as shown in Fig. 6). Misconduct is by the use of a conditional check. when a trigger occurs the blockchain records an action, verifies it, and genuineness are assessed in light of Ui's prior consent decision (granted/denied) for that consent. using RFi . SC2 is reliant on three input variables: transactions that were started from FPi or Ri the results of SC1, and

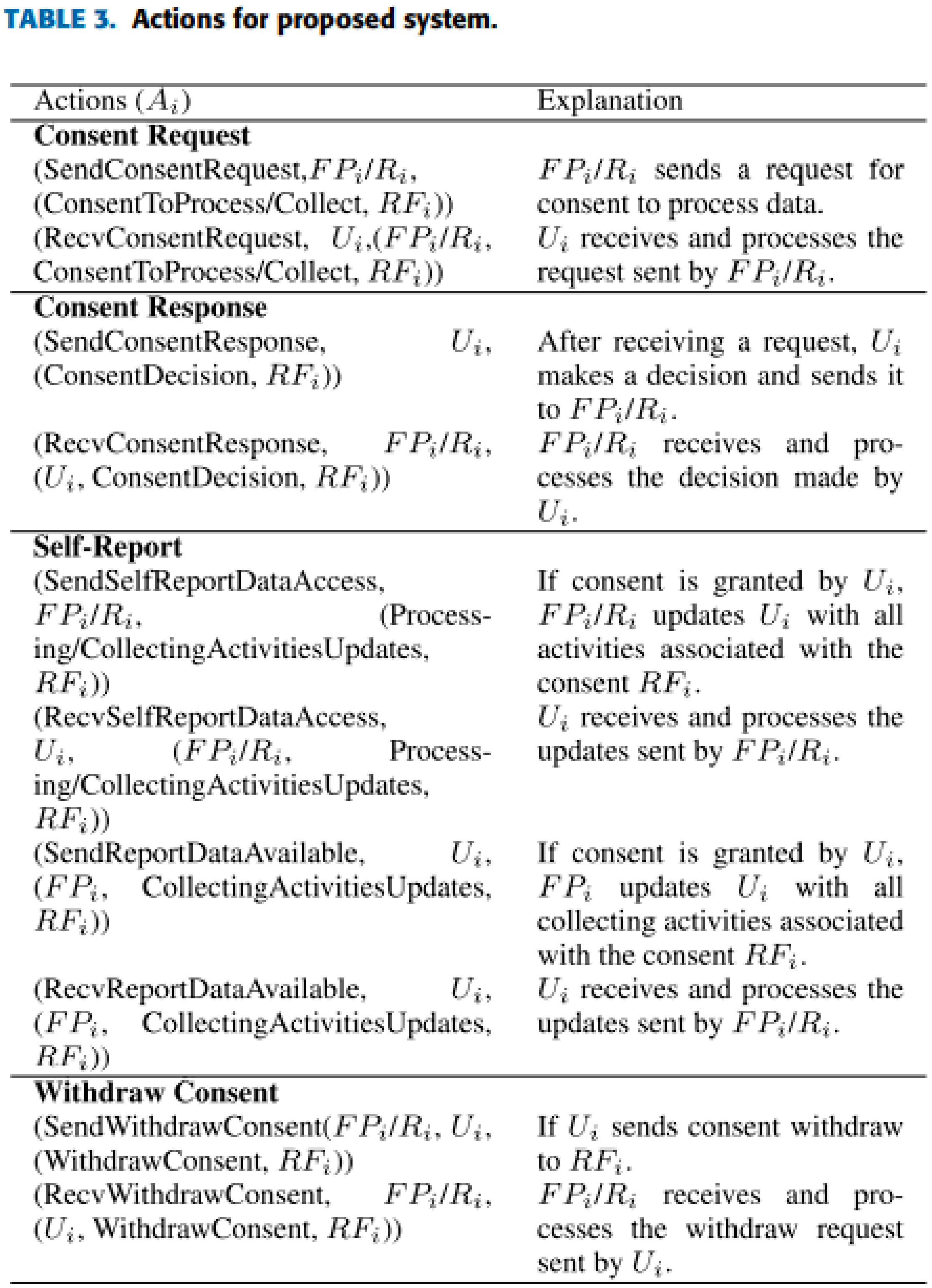


TABLE 3. Actions for proposed system.

Actions (A_i)	Explanation
Consent Request	
(SendConsentRequest,FP_i/R_i, (ConsentToProcess/Collect, RF_i))	FP_i/R_i sends a request for consent to process data.
(RecvConsentRequest, U_i,(FP_i/R_i, ConsentToProcess/Collect, RF_i))	U_i receives and processes the request sent by FP_i/R_i.
Consent Response	
(SendConsentResponse, U_i, (ConsentDecision, RF_i))	After receiving a request, U_i makes a decision and sends it to FP_i/R_i.
(RecvConsentResponse, FP_i/R_i, (U_i, ConsentDecision, RF_i))	FP_i/R_i receives and processes the decision made by U_i.
Self-Report	
(SendSelfReportDataAccess, FP_i/R_i, (Processing/CollectingActivitiesUpdates, RF_i))	If consent is granted by U_i, FP_i/R_i updates U_i with all activities associated with the consent RF_i.
(RecvSelfReportDataAccess, U_i, (FP_i/R_i, Processing/CollectingActivitiesUpdates, RF_i))	U_i receives and processes the updates sent by FP_i/R_i.
(SendReportDataAvailable, U_i, (FP_i, CollectingActivitiesUpdates, RF_i))	If consent is granted by U_i, FP_i updates U_i with all collecting activities associated with the consent RF_i.
(RecvReportDataAvailable, U_i, (FP_i, CollectingActivitiesUpdates, RF_i))	U_i receives and processes the updates sent by FP_i/R_i.
Withdraw Consent	
(SendWithdrawConsent(FP_i/R_i, U_i, (WithdrawConsent, RF_i))	If U_i sends consent withdraw to RF_i.
(RecvWithdrawConsent, FP_i/R_i, (U_i, WithdrawConsent, RF_i))	FP_i/R_i receives and processes the withdraw request sent by U_i.

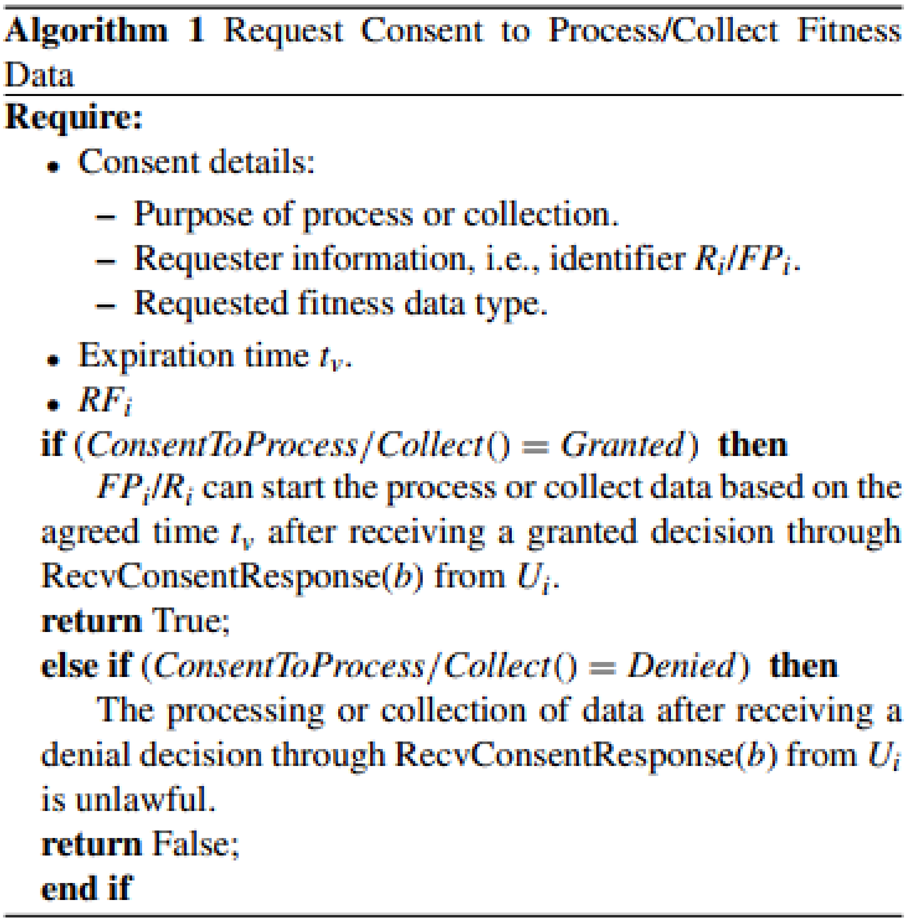
Figure 3.4: Actions for proposed system

the documented Ui's approval to the denial. The designation of The RFi reference number is consent. Below, we formally state the design objectives based on the attributes of SC2:

- **DG4** Due to Ui's expressed authorization, the FPi processed data have to be real for Ui.
- **DG5** Based on Ui's expressed assent, the Ri-collated data must be accurate for Ui.

3.6 Algorithms

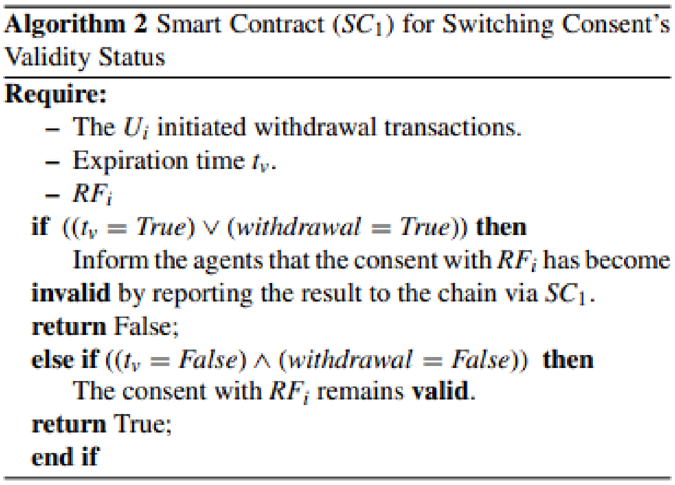
3.6.1 Algorithm 1 Ask for permission to process or collect fitness data.



```
Algorithm 1 Request Consent to Process/Collect Fitness Data
Require:
  • Consent details:
      – Purpose of process or collection.
      – Requester information, i.e., identifier $R_i/FP_i$.
      – Requested fitness data type.
  • Expiration time $t_v$.
  • $RF_i$
  if ($ConsentToProcess/Collect() = Granted$) then
      $FP_i/R_i$ can start the process or collect data based on the
  agreed time $t_v$ after receiving a granted decision through
  RecvConsentResponse($b$) from $U_i$.
  return True;
  else if ($ConsentToProcess/Collect() = Denied$) then
      The processing or collection of data after receiving a
  denial decision through RecvConsentResponse($b$) from $U_i$
  is unlawful.
  return False;
  end if
```

Figure 3.5: Algorithm 1

3.6.2 Algorithm 2 Smart Contract (SC1) for Switching Consent's Validity

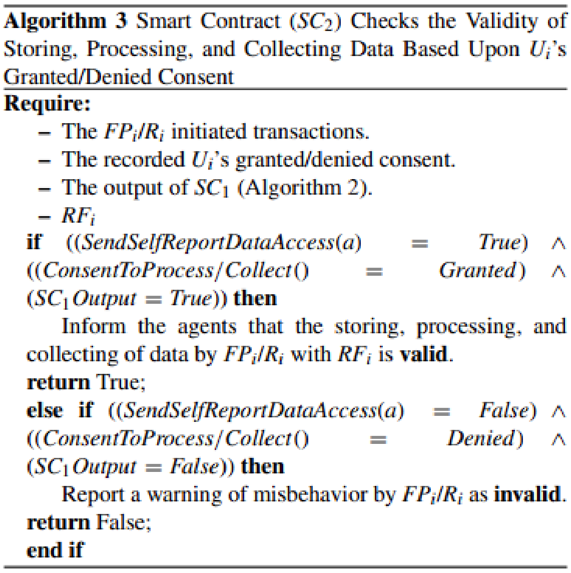


Algorithm 2 Smart Contract (SC_1) for Switching Consent's Validity Status

```
Require:
  – The $U_i$ initiated withdrawal transactions.
  – Expiration time $t_v$.
  – $RF_i$
  if (($t_v = True$) $\vee$ ($withdrawal = True$)) then
      Inform the agents that the consent with $RF_i$ has become invalid by reporting the result to the chain via $SC_1$.
  return False;
  else if (($t_v = False$) $\wedge$ ($withdrawal = False$)) then
      The consent with $RF_i$ remains valid.
  return True;
  end if
```

Figure 3.6: Algorithm 2

3.6.3 Algorithm 3 Smart Contract (SC2) Examines the accuracy of data storage, processing, and collection based on the user's granted or denied consent.



Algorithm 3 Smart Contract (SC_2) Checks the Validity of Storing, Processing, and Collecting Data Based Upon U_i's Granted/Denied Consent

```
Require:
  – The $FP_i/R_i$ initiated transactions.
  – The recorded $U_i$'s granted/denied consent.
  – The output of $SC_1$ (Algorithm 2).
  – $RF_i$
  if (($SendSelfReportDataAccess(a) = True$) $\wedge$ (($ConsentToProcess/Collect() = Granted$) $\wedge$ ($SC_1 Output = True$)) then
      Inform the agents that the storing, processing, and collecting of data by $FP_i/R_i$ with $RF_i$ is valid.
  return True;
  else if (($SendSelfReportDataAccess(a) = False$) $\wedge$ (($ConsentToProcess/Collect() = Denied$) $\wedge$ ($SC_1 Output = False$)) then
      Report a warning of misbehavior by $FP_i/R_i$ as invalid.
  return False;
  end if
```

Figure 3.7: Algorithm 3

Chapter 4

EXPERIMENTAL STUDY

4.1 Putting Security Requirements in Writing

SeMF, created by authors, is what we utilise for formal system modelling. and verification of the proposed system's security features. Formal language theory, which models objects in fine-grained ways, serves as the foundation for this approach. the system's specifications and characteristics. A thorough explanation of SeMF, which is outside the purview of This study is documented. We utilise SeMF's in this area. the formalisation of the security needs' formal definitions a few of the suggested system model specifications. These The two conditions for security are (A) authenticity and (B) proof. (with integrity and authorization qualities) of authenticity implied during the conversation).

4.2 Authentication

4.2.1 Definition of the Property

By confirming the communicators' identities, authentication shows that they are who they say they are. In order to formalise the authenticity feature presented in Section IV, we employ Definitions 1 and 2 from SeMF [18].

4.2.2 Formalize Authenticity of Actions

The blockchain type employed in the suggested system is a permissioned blockchain, in which players are added by RA. Outside of the suggested system model, the process of adding members entails RA validating their true identities before releasing key pairs for blockchain accounts. We consider that all players were authenticated and validated by the RA before they joined the system under the proposed system model. The first transaction is always signed using skP whenever some agent have to insert something into the blockchain. Later, the blockchain uses its pkP to validate the transaction. Because only one agent, a distributed system (the blockchain), which is not a single entity, verifies the authenticity, the system does not require a global Public Key Infrastructure (PKI) where everyone believes the key. All agents can determine whether a system action is genuine and comes from the intended agent thanks to Assumptions 7 and 8.

4.2.3 End to End Authentication Trust

An end device or account must typically be used to confirm a digital signature, which Agent P cannot do on their own. As a result, the agent accounts rather than the agents P or their end devices are used to determine the authenticity. According to Assumption 4, a blockchain network serves as the component of the proposed system that conducts the authentication validation check. As a result, the blockchain only accepts signed, legitimate transactions that have the right skP and verifies the transaction's origin. As shown in Fig. 10, each agent P in the system has a blockchain account or set of accounts made up of pkP and skP pairs. Ai for the blockchain to confirm the authenticity of the additional action Ai taken by agent P on the blockchain and that it was in fact produced by that agent.

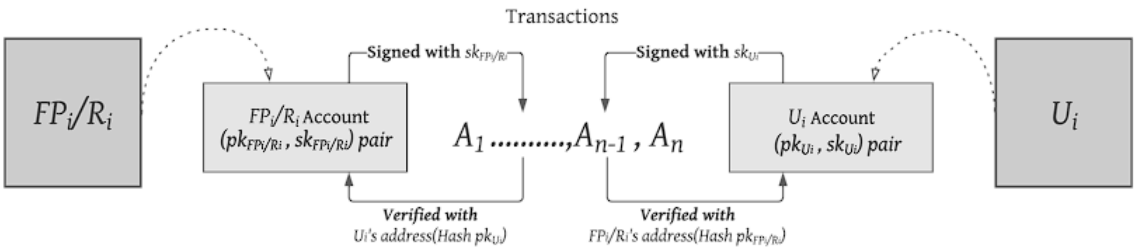

Transactions
Signed with sk_{FP_i/R_i}
Signed with sk_{U_i}
FP_i/R_i
FP_i/R_i Account
(pk_{FP_i/R_i}, sk_{FP_i/R_i}) pair
A_1.........,A_{n-1} , A_n
U_i Account
(pk_{U_i}, sk_{U_i}) pair
U_i
Verified with
U_i's address(Hash pk_{U_i})
Verified with
FP_i/R_i's address(Hash pk_{FP_i/R_i})

FIGURE 10. End-to-end authentication trust.

Figure 4.1: End-to-end authentication trust

4.2.4 Original Communication

Every agent in the system has a unique P and can only view their own sent or received activities. A1. . .An. A1 can be used to represent Auth to determine the veracity of submitted and received activities (a, b, P). In other words, agent P must be able to authenticate that action a has already happened if a certain action b has occurred in a series of acts. A clear description of what "genuine" implies is therefore necessary in order to confirm the validity of these actions. The SeMF's [18] definitions 1 and 2 are used as a result.

4.2.5 Smart Contract SC1's Proof

By using this procedure, the granted consent decision will either be rendered void if it has been revoked or valid for a set length of time. The intended system Design Goal DG 3 is supported by the system according to Proof 2. This can be said in the following way.

$$\begin{aligned}&auth(auth(sendWithdrawConsen(WithdrawConsent,\\&\quad RF_i), recvWithdrawConsen(WithdrawConsent, RF_i),\\&\quad FP_i/R_i) \vee\ auth(t_v(expired), RF_i), \mathbb{P})\end{aligned} \qquad (5)$$

Figure 4.2: Smart Contract 1

4.2.6 Smart Contract SC2's Proof

This agreement tries to evaluate the legality of data collection, processing, and storage based on Ui's granted or withheld consent. The proposed system Design Goal, DG 5, is supported by the system according to Proof 2. This can be said in the following way.

$$\begin{aligned}&auth(auth(sendReportDataAvailable(ConsentToCollect,\\&\quad RF_i), recvReportDataAvailable(ConsentToCollect,\\&\quad RF_i), U_i) \wedge\ auth(sendConsentResponse\\&\quad (ConsentDecision, RF_i), recvConsentResponse\\&\quad (ConsentDecision, RF_i), FP_i/R_i) \wedge\ auth(SC_1 results,\\&\quad RF_i), \mathbb{P}) \qquad (6)\end{aligned}$$

Figure 4.3: Smart Contract 2

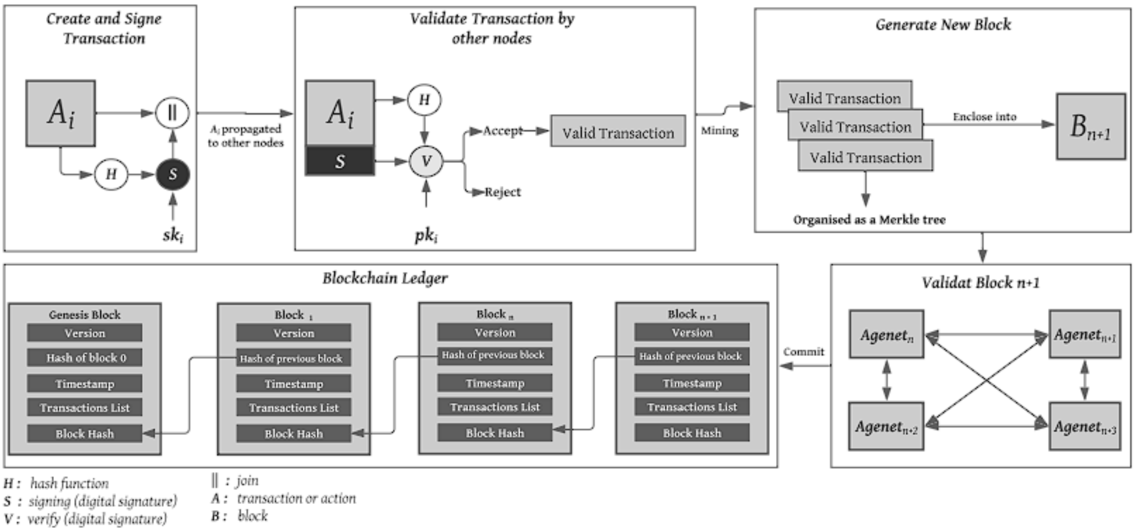


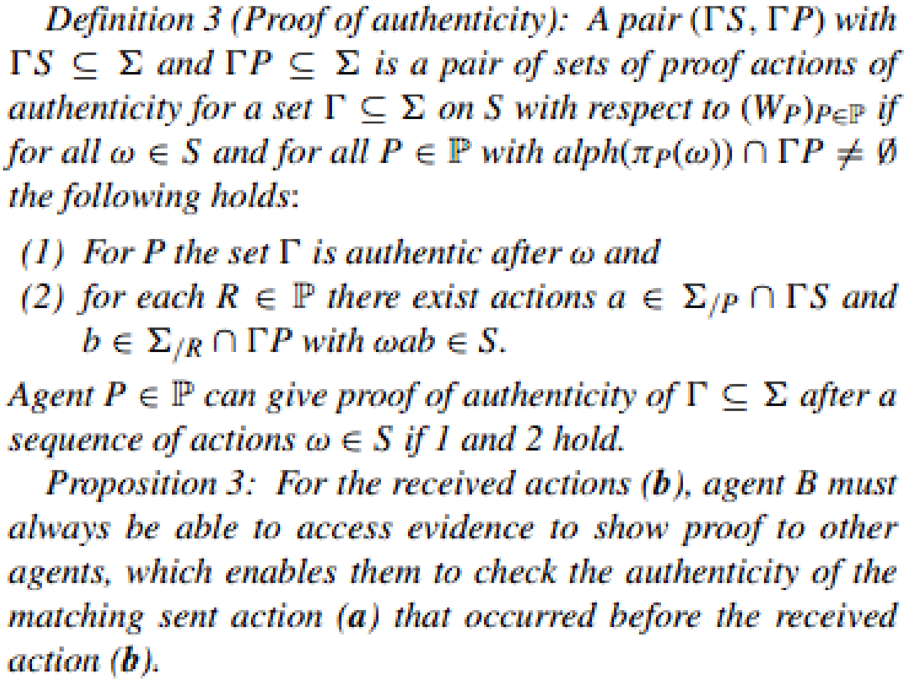
FIGURE 15. Blockchain's built-in approaches to guarantee nonrepudiation.

Figure 4.4: The methods built into blockchain technology to ensure nonrepudiation..

4.3 AUTHENTICITY PROOF

4.3.1 Describing the Property

Two communication pairs are involved in this property, and neither the transmitted nor the received transactions may be disputed. We formalise the proof of authenticity attribute introduced in Section IV using the definition from SeMF [18]:



Definition 3 (Proof of authenticity): A pair $(\Gamma S, \Gamma P)$ *with* $\Gamma S \subseteq \Sigma$ *and* $\Gamma P \subseteq \Sigma$ *is a pair of sets of proof actions of authenticity for a set* $\Gamma \subseteq \Sigma$ *on S with respect to* $(W_P)_{P \in \mathbb{P}}$ *if for all* $\omega \in S$ *and for all* $P \in \mathbb{P}$ *with* $alph(\pi_P(\omega)) \cap \Gamma P \neq \emptyset$ *the following holds:*

(1) For P the set Γ *is authentic after* ω *and*

(2) for each $R \in \mathbb{P}$ *there exist actions* $a \in \Sigma_{/P} \cap \Gamma S$ *and* $b \in \Sigma_{/R} \cap \Gamma P$ *with* $\omega ab \in S$.

Agent $P \in \mathbb{P}$ *can give proof of authenticity of* $\Gamma \subseteq \Sigma$ *after a sequence of actions* $\omega \in S$ *if 1 and 2 hold.*

*Proposition 3: For the received actions (**b**), agent B must always be able to access evidence to show proof to other agents, which enables them to check the authenticity of the matching sent action (**a**) that occurred before the received action (**b**).*

Figure 4.5: Authenticity Proof

4.3.2 Formalize the Authenticity Proof for Actions

The usage of blockchain as an evidence recorder, where all consent-related activity records and transaction are entered and resolved permanently into a shared ledger, is a great way to handle this security feature. According to Assumption, a blockchain is made up of a series of interconnected blocks, each of which adds links to its immediate predecessors up until the so-called genesis block, which has index 0. According to Assumption 8, each entity receives a copy of all the records, which are kept as chronologically unalterable records and connected by hash values. Effective ways to ensure nonrepudiation include digital signature schemes (asymmetric encryption), timestamps, and the immutability of records, which enables the system's steps to be traced for authenticity verification.

4.4 Results Analysis

The proposed system security requirements are interpreted in this study's verbal descriptions, and then these requirements are formalised using the SeMF tool. The research results presented in this paper are simply the first phase in creating blockchain-based consent management. The usefulness of the suggested model in terms of the computing, storage, and communication overhead of each entity will be demonstrated in subsequent work through the use of an experimental evaluation. Further investigation is also required to decide which blockchain-related technical features, such as the consensus algorithm, the use of tokens and their economics, and the procedure for identifying fitness devices, are appropriate for the proposed solution.

Chapter 5

CONCLUSION

There are various privacy issues with disclosing personal fitness information to outside parties. This study aims to solve these issues in the privacy policies of fitness trackers by giving users more control over how their fitness data is processed. To address difficulties with privacy preservation, we created a dynamic consent method based on blockchain. The formal proof model, requirements specification, and system architecture are the main artefacts in the suggested system. This study additionally assesses the identified blockchain assumptions and the demonstrated artefacts using the SeMF tool. The SeMF evaluation demonstrates that the system achieves all of our design objectives as a consequence. By enhancing user control over the processing of fitness data, we get to the conclusion that the suggested method is suitable for protecting user privacy. Further study is necessary to close the remaining gap, which is that fitness trackers must accurately send their real processing actions to the blockchain.

In this study, verbal descriptions of the proposed system security needs are translated into formal obligationss using the SeMF tool. The research presented in this paper just represents the initial stages of creating a blockchain-based consent management system. In our upcoming study, we intend to carry out an experimental evaluation to show how well the suggested model reduces the computing, storage, and communication overhead of each entity. Further investigation is also required to discover the best blockchain-related technical choices for the suggested solution, including but not restricted to the concord algorithm, token usage and economics, and fitness device authentication technique.

REFERENCES

1. L. Hutton, B. A. Price, R. Kelly, C. McCormick, A. K. Bandara, T. Hatzakis, M. Meadows, and B. Nuseibeh, "Assessing the privacy of mHealth apps for self-tracking: Heuristic evaluation approach," JMIR mHealth uHealth, vol. 6, no. 10, p. e185, Oct. 2018.

2. R. K. Saripalle, "Leveraging FHIR to integrate activity data with electronic health record," Health Technol., vol. 10, pp. 341–352, Apr. 2019.

3. K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," J. Manage. Inf. Syst., vol. 24, no. 3, pp. 45–77, 2007.

4. R. Sallis, "Developing healthcare systems to support exercise: Exercise as the fifth vital sign," Brit. J. Sports Med., vol. 45, no. 6, pp. 473–474, 2011.

5. M. M. Madine, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, S. Ellahham, and P. Calyam, "Fully decentralized multi-party consent management for secure sharing of patient health records," IEEE Access, vol. 8, pp. 225777–225791, 2020.

6. J. Ahmed, S. Yildirim, M. Nowostaki, R. Ramachandra, O. Elezaj, and M. Abomohara, "GDPR compliant consent driven data protection in online social networks: A blockchain-based approach," in Proc. 3rd Int. Conf. Inf. Comput. Technol. (ICICT), Mar. 2020, pp. 307–312.

7. Q. Grundy, F. P. Held, and L. A. Bero, "Tracing the potential flow of consumer data: A network analysis of prominent health and fitness apps," J. Med. Internet Res., vol. 19, no. 6, p. e233, Jun. 2017.

8. M. Hatamian, J. Serna, and K. Rannenberg, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets," Comput. Secur., vol. 83, pp. 332–353, Jun. 2019.

9. N. Momen, M. Hatamian, and L. Fritsch, "Did app privacy improve after the GDPR?" IEEE Secur. Privacy, vol. 17, no. 6, pp. 10–20, Nov. 2019.

10. G. Despotou, J. Evans, W. Nash, A. Eavis, T. Robbins, and T. N. Arvanitis, "Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study," Digit. Health, vol. 6, Mar. 2020, Art. no. 2055207620924949

11. R. Neisse, G. Baldini, G. Steri, Y. Miyake, S. Kiyomoto, and A. R. Biswas, "An agent-based framework for informed consent in the Internet of Things," in Proc. IEEE 2nd World Forum Internet Things (WFIoT), Dec. 2015, pp. 789–794.

12. D. Peras, "Guidelines for GDPR compliant consent and data management model in ICT businesses," in Proc. Central Eur. Conf. Inf. Intell. Syst., 2018, pp. 113–121.

13. A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl, “Availability and quality of mobile health app privacy policies,” J. Amer. Med. Inform. Assoc., vol. 22, no. e1, pp. e28–e33, Apr. 2015.

14. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Oct. 2017, pp. 1–5.

15. S. Gilda and M. Mehrotra, “Blockchain for student data privacy and consent,” in Proc. Int. Conf. Comput. Commun. Informat. (ICCCI), Jan. 2018, pp. 1–5.

16. Strava. (2020). Strava Privacy Policy. [Online]. Available: https://www.strava.com/legal/privacyfull_policy

17. K. Rantos, G. Drosatos, A. Kritsas, C. Ilioudis, A. Papanikolaou, and A. P. Filippidis, “A blockchain-based platform for consent management of personal data processing in the IoT ecosystem,” Secur. Commun. Netw., vol. 2019, pp. 1–15, Oct. 2019.

18. A. Fuchs, S. Gurgens, and C. Rudolph, “A formal notion of trust–enabling reasoning about security properties,” in Proc. IFIP Int. Conf. Trust Manage. Berlin, Germany: Springer, 2010, pp. 200–215.

19. A. Pfitzmann and M. Hansen. (Aug. 2010). A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. v0.34. [Online]. Available: http://dud.inf. tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

20. OAIC. (2018). Australian Entities and the EU General Data Protection Regulation GDPR. [Online]. Available: https://www.oaic.gov.au/ privacy/guidance-and-advice/australian-entities-and-the-eu-generaldata-protection-regulation

21. A. Troiano, “Wearables and personal health data: Putting a premium on your privacy,” Brooklyn Law Rev., vol. 82, no. 4, p. 1715, 2016. [Online]. Available: https://heinonline.org/HOL/P?h=hein. journals/brklr82i=1759

22. M. Kang and V. Lemieux, “A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage,” Ledger, vol. 6, Nov. 2021.

23. P. V. Kakarlapudi and Q. H. Mahmoud, “A systematic review of blockchain for consent management,” Healthcare, vol. 9, no. 2, p. 137, Feb. 2021.

24. P. Genestier, S. Zouarhi, P. Limeux, D. Excoffier, A. Prola, S. Sandon, and J.-M. Temerson, “Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges,” J. Int. Soc. Telemed. eHealth, vol. 5, pp. GKR–e24, 2017.

25. K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, E. G. Teo, and C. H. Suen, “Double-blind consent-driven data sharing on blockchain,” in Proc. IEEE Int. Conf. Cloud Eng. (IC2E), Apr. 2018, pp. 385–391

26. T. Rupasinghe, “Blockchain-based dynamic consent for secondary use of electronic medical records,” Ph.D. dissertation, Dept. Softw. Syst. Cybersecur., Monash Univ., Melbourne, VIC, Australia, 2021.

27. D. M. Maslove, J. Klein, K. Brohman, and P. Martin, “Using blockchain technology to manage clinical trials data: A proof-of-concept study,” JMIR Med. Informat., vol. 6, no. 4, Dec. 2018, Art. no. e11949.

28. S. Breen, K. Ouazzane, and P. Patel, “GDPR: Is your consent valid?” Bus. Inf. Rev., vol. 37, no. 1, pp. 19–24, Mar. 2020.

29. W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, “Digital signature scheme for information non-repudiation in blockchain: A state of the art review,” EURASIP J. Wireless Commun. Netw., vol. 2020, no. 1, pp. 1–15, Dec. 2020

30. G. Despotou, J. Evans, W. Nash, A. Eavis, T. Robbins, and T. N. Arvanitis, “Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the Dovetail digital consent application: A cross sectional exploratory study,” Digit. Health, vol. 6, Mar. 2020, Art. no. 2055207620924949.