PLOS ONE

RESEARCH ARTICLE

Blockchain-secure patient Digital Twin in healthcare using smart contracts

Sandro Amofa, Qi Xia, Hu Xia, Isaac Amankona Obiri, Bonsu Adjei-Arthur, Jingcong Yang, Jianbin Gao*

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

* gaojb@uestc.edu.cn

Citation: Amofa S, Xia Q, Xia H, Obiri IA, Adjei-Arthur B, Yang J, et al. (2024) Blockchain-secure patient Digital Twin in healthcare using smart contracts. PLoS ONE 19(2): e0286120. https://doi.org/10.1371/journal.pone.0286120

Editor: Omar A. Alzubi, Al-Balqa Applied University Prince Abdullah bin Ghazi Faculty of Information Technology, JORDAN

Received: January 4, 2023

Accepted: April 25, 2023

Published: February 29, 2024

Data Availability Statement: We do not know of specific legal reasons to completely bar us from sharing data with other researchers for the purposes of scientific inquiry. However, in all our research we are guided by healthcare privacy regulations HIPAA, HITECH, and others as they apply so as to avoid legal challenges altogether. The dataset can be made available on request. To place a request, please send an email to that effect to 202124080119@std.uestc.edu.cn, Graduate Student Researcher: He is the Curator for this research.

Abstract

Modern healthcare has a sharp focus on data aggregation and processing technologies. Consequently, from a data perspective, a patient may be regarded as a timestamped list of medical conditions and their corresponding corrective interventions. Technologies to securely aggregate and access data for individual patients in the quest for precision medicine have led to the adoption of Digital Twins in healthcare. Digital Twins are used in manufacturing and engineering to produce digital models of physical objects that capture the essence of device operation to enable and drive optimization. Thus, a patient's Digital Twin can significantly improve health data sharing. However, creating the Digital Twin from multiple data sources, such as the patient's electronic medical records (EMR) and personal health records (PHR) from wearable devices, presents some risks to the security of the model and the patient. The constituent data for the Digital Twin should be accessible only with permission from relevant entities and thus requires authentication, privacy, and provable provenance. This paper proposes a blockchain-secure patient Digital Twin that relies on smart contracts to automate the updating and communication processes that maintain the Digital Twin. The smart contracts govern the response the Digital Twin provides when queried, based on policies created for each patient. We highlight four research points: access control, interaction, privacy, and security of the Digital Twin and we evaluate the Digital Twin in terms of latency in the network, smart contract execution times, and data storage costs.

1 Introduction

A Digital Twin is a data-driven model of a physical asset, process, or system [1] with a persistent data connection between the physical object and model. This enables sensory data from the physical object to create increasingly detailed virtual models that reveal detective, preventative, or corrective insights for optimized operations [2]. There are several benefits to Digital Twins and the barrier to their creation is getting lower by the day due to the availability of digital tools for data collection and analytics, increasing computing power, and diminishing costs of cloud data storage.

Digital Twins are used in manufacturing for quality control and optimization purposes [3] where they permit virtual objects to be created and tested by subjecting them to exploitative,

Funding: This research was funded by the Basic Strengthening Program (2021- JCJQ-JJ-0463), the scientific and technological innovation talents of Sichuan Province (2023JDRC0001), the National Natural Science Foundation of China (No. U22B2029), Shenzhen Research Program (No. JSGG20210802153537009).

Competing interests: The authors of the article declare that there are no competing interests.

destructive experiments which may not be permitted in the physical world due to prohibitive financial costs, ethical or legal implications, etc. [4]. Thus, the application of Digital Twin technology to healthcare can bring many benefits, as experiments can be performed on data models to determine optimal treatments before prescribing them to the patient. Using available patient electronic medical records, data from smart devices, computing power, and analytics algorithms, a Digital Twin can be created for the patient, as shown in Fig 1. With more data, better approximations of the patient Digital Twin can be produced and queried to provide better access to healthcare at reduced costs and enable a higher quality of life for patients.

However, Digital Twins raise difficult questions regarding security and privacy [5]. The data connection between the patient and the Digital Twin creates the computational model of the patient's condition(s). Inevitably, without adequate security, inaccurate data input to the Digital Twin can have serious consequences for the patient since his/her treatment may be based on the output the Digital Twin demonstrates. Additionally, unauthorized access to the Digital Twin can reveal compromising details about the patient that may cause long-term damage to their reputation with adverse financial consequences. Hence, it is critical to demand guarantees on the security of the Digital Twin and also to restrict the information it provides when queried. This research proposes a mechanism to handle four key research points: access control, interaction, privacy, and security of the Digital Twin. The need for secure data, reliable storage, trusted computing and other cooperative mechanisms with mutually beneficial interactions can be addressed using the blockchain [6–9] where a network of institutions and users collaborate to share data, collectively confer consensus-based validity on transactions, and

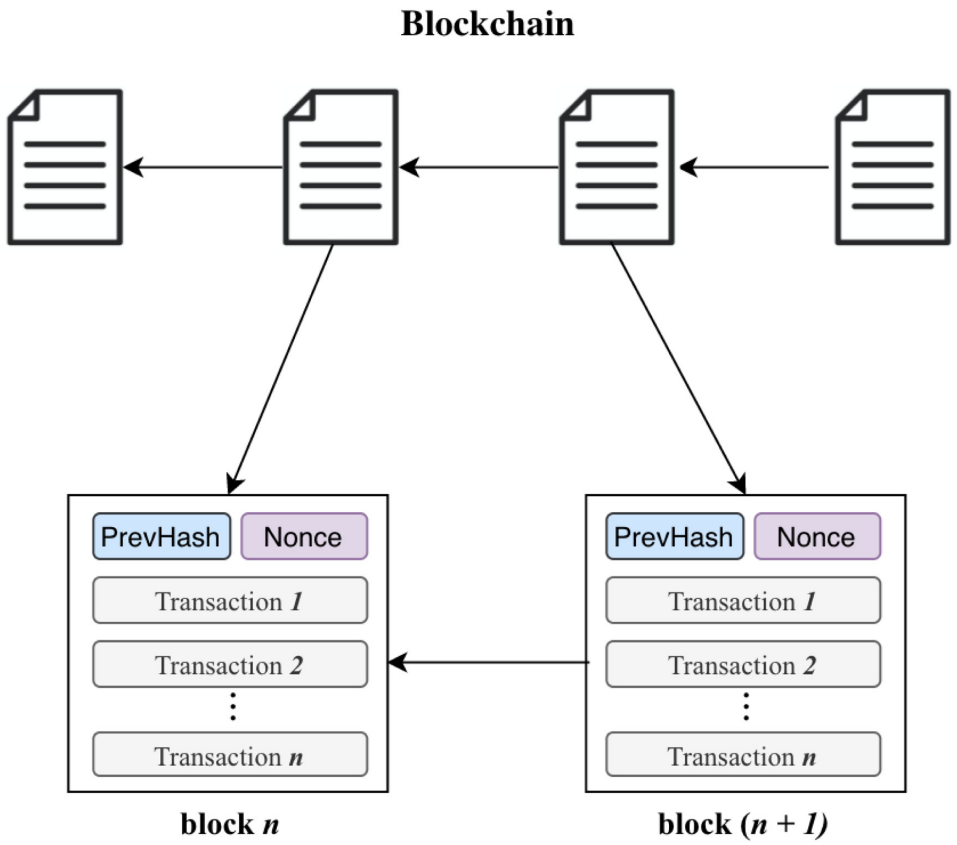

Fig 1. Digital Twin instances from multi-data sources.

https://doi.org/10.1371/journal.pone.0286120.g001

maintain a single coherent transactions history. Provenance of data and transactions can also be guaranteed since the blockchain provides rigorous mechanisms for data integrity using digital signatures and cryptographic hashes with timestamps [10]. Periodic updates are critical for Digital Twins, thus it is important to set limits on the data the Digital Twin can receive or provide when queried. Hence, we propose a blockchain-based Digital Twin that can model the individual patient's condition(s) and facilitate care by accessing specific services. We employ a suite of smart contracts to mediate access to the data stores from which the Digital Twin is updated.

1.1 Contribution

We outline our main contribution to the use of Digital Twins in healthcare below:

1. We present an automated, blockchain-based patient Digital Twin that uses smart contracts to mediate access to the Digital Twin and control its interactions.
2. We present a mathematical model of the patient Digital Twin defining it with a focus on timestamped instances.
3. We present a novel Multi-receiver Identity-Based Signcryption (mIBSC) scheme to secure the patient Digital Twin which has a constant ciphertext size and an element that can be stored on the blockchain to prove the authorship of digital twin.

The remainder of the paper is organized as follows: Section 2 presents Related Works while Section 3 provides Preliminaries dealing with the Blockchain, Digital Twins and cryptographic assumptions. Section 4 deals with the System Overview and component interactions. Section 5 discusses System Design and Section 6 presents Security proofs for our research. Section 7 provides the Efficiency Evaluation of the computations implemented and some metrics. Section 8 concludes the research and offers directions for future works.

2 Related works

In this section we review Digital Twins usage in healthcare with a focus on secure patient data sharing using smart contracts. In [11], the authors continuously monitor patients' conditions and improve patient outcomes, quality of life and reduce financial costs by using Digital Twin technology for healthcare. According to this research, health monitoring can be achieved using wearable sensors for early detection of worsening health or manage chronic conditions. Furthermore, assistive technologies and increasing usage of real-time data can enable new and dynamic health services with minimal risk for the patient. The research also proposes fast simulations of conditions using machine learning for accurate crisis prediction. Thus, doctors can use the patient's Digital Twin as a planning tool for intelligent control and emergency response. In [12], the authors define questions surrounding the materialisation, expectation and the implementation of Digital Twins in healthcare. They conclude Digital Twins can provide a useful test platform for enabling preventive healthcare for patients through simulations that employ trial-and-error so that consequences of given treatments can be evaluated empirically before the actual treatment is administered to patients. This provides a cost-effective implementation of precision medicine that offers patients the possibility of personalized treatments. For [13], the researchers tackle the integration of Digital Twins with agents and multi-agent systems. They focused on the design of agent-based Digital Twins and their utility in the context of healthcare management. They highlight the importance of Digital Twins using a case study where contextual Digital Twins of a trauma victim alert emergency medical staff in a hospital with vital details about the incoming

patient. The authors of A Blockchain-based Secure Digital Twin Framework for Smart Healthy City propose a Digital Twin framework that consists of three layers: a Device Layer, a Blockchain Layer and an Application Layer. They discuss the application of their framework to the COVID-19 pandemic and highlight its suitability for use with other future public health emergencies. It provided a sequence diagram that shows how two Digital Twins and a hospital could collaborate to exchange public keys necessary for notification in case of confirmed infection. However, they do not provide proof for encryption and other security-related algorithms necessary to protect a Digital Twin [14]. This article [15] is concerned with the lack of a data collection mechanism that adequately addresses the challenge of fusing data from multiple disparate sources. The research then describes a concrete computational model of a Digital Twin for healthcare, proposes a Healthcare Digital Twin (HDT) system, and defines the protocol progression for the framework that corresponds to the mathematical model. Being a conceptual model, it provides no experimental results for any of the interactions of the Digital Twins.

We considered [16–19] for their insights on coupling Digital Twins with blockchain technology. While we appreciate their views, they do not apply to healthcare or patients. The literature agrees that the security of the Digital Twin is essential. Still, there are few proposals on guaranteeing the patient Digital Twin's privacy and security. Thus, our research uses smart contracts to mediate access to and control of the patient's Digital Twin.

2.1 Broadcast encryption

Fiat and Naor first introduced the concept of broadcast encryption (BE) or multi-receivers encryption in [20]. They proposed a method for securely encrypting a message for a group of users so that only those in the group could decrypt it. On the other hand, a coalition of non-set users cannot obtain any information about the broadcast message. Many BE methods have been developed in the contexts of identity-based encryption [21–23] and standard public-key encryption [24]. Delerablée [21] introduced the first identity-based broadcast encryption (IBBE) system with constant-size ciphertexts and private keys in the identity-based encryption context. The approach, however, does not provide ciphertext authentication. The properties of authentication and secrecy are both necessary for sharing sensitive data, such as electronic medical data. BE with source authentication is also called authenticated BE or broadcast signcryption. Selvi et al. [25] proposed an efficient identity-based signcryption scheme in this area. Similar to broadcast signcryption, there have been several multi-receiver signcryption schemes [26, 27], where the ciphertexts are of a size linear in the number of the set of receivers. Broadcast authentication schemes have also been proposed without supporting the confidentiality of the broadcast message in the public key setting [23]. Recently, Yang et al. [28] proposed a multi-message and multi-receiver signcryption scheme based on blockchain. The scheme enables medical data providers to send messages to multiple data requesters by executing one signcryption operation, which satisfies the multi-message sending requirements of the data providers in the communication environment. However, the ciphertexts are linear in the number of sets of receivers. Note that our case requires that the data owner use the blockchain to track the sequence of the patient's Digital Twin data so that each care provider can ascertain the progress of the patient's health. The proposed solution requires a constant ciphertext size and an element that can be stored on the blockchain to prove the authorship of data encryption. The existing multi-receiver signcryption does not appear relevant to our scenario. Therefore, the proposed multi-receiver signcryption has a constant ciphertext size with a small size of elements that can be stored on the blockchain to determine the sequence and authorship of the ciphertext.

Table 1. Comparison of reviewed literature with proposed solution.

Reference	Limitations	Our work
[15]	Does not specify model for data sharing	Provides one-to-one/many model for data sharing
	Does not provide any experimental results	Provides experimental results on operations/costs
	Unclear explanation of blockchain implementation.	Provides clear implementation of blockchain and operations
	Stores raw data off-chain	Stores only encrypted health records
	Seeks to virtualize healthcare as a service	Provides the digital twin to access services and data.
[29]	Work is not applicable to healthcare	Presents a digital twin that is healthcare-inclined
	No data confidentiality, a key point of health data sharing	Preserves confidentiality & integrity required in health data sharing
	No description of security parameters for storage of files.	Adequately describes the security for stored files
[30]	Uses symmetric encryption with no support for one-to-many sharing	Uses mIBSC encryption which supports one-to-many sharing
	Does not provide integrity controls for off-chain data storage	Uses inherent blockchain integrity controls
[31]	Focused on securing health data sharing between individual patients	Provides a digital twin that supports multiple user access
	Uses anonymity as a key security metric.	Requires identity for digital twin creation and usage
[24]	Does not protect data integrity, essential for secure data transactions	Guarantees data integrity, scheme thrives on signcryption & blockchain.
	Not applicable to health data sharing as there is no system model	Provides a system model, digital twin can access data/services.
	Protocol also lack verification.	Verification of protocol
[26]	Ciphertext sizes grow linearly with increasing number of receivers	Maintains static ciphertext size irrespective of no. of receivers
		Reduces communication and computation costs.
	Not applicable to data sharing as there is no system model	Provides system model, digital twin can securely access data
[28]	Ciphertext sizes grow linearly with increasing number of receivers	Maintains static ciphertext size irrespective of size of no. of receivers
		Reduces communication and computation costs.
	Not applicable to digital twin operations such as data contracts and service contracts.	Is based on digital twin operations.
	No sequential ordering for tracking digital twin authorship	Provides digital twin authorship tracking to check patient progress and completeness of patient data.

https://doi.org/10.1371/journal.pone.0286120.t001

Table 2. A comparison of some state-of-the-art Digital Twin research papers in healthcare.

	[11]	[12]	[13]	[14]	[15]
Focus	Mo	IMP	Integration	Public health management	Structured data aggregation
Utility	SI	SI	Strategic care planning	Pandemic control (Covid-19)	Secure health data storage
Paradigm	PM	PC	Multi-agent systems	Smart City health	Multi-agent systems
Security	NP	NP	NP	NP	AP
Privacy	NP	NP	NP	NP	AP
Framework	NP	NP	Agent-based	Blockchain-based	Blockchain-based

AP = Applicable, NP = Non-applicable, Mo = Monitoring, PM = Precision medicine, Imp = Implementation, SI = Simulation, PC = Preventive care

https://doi.org/10.1371/journal.pone.0286120.t002

Table 1 presents a summary of related work and identified research gaps, while Table 2 compares state-of-the-art research papers in digital twin technology applied to healthcare, categorized by focus, utility, paradigm, security, privacy, and framework. This comprehensive and well-organized overview of research papers serves as a valuable reference for understanding the various areas of focus and approaches in the digital twin field applied to healthcare.

3 Preliminaries

This section presents Digital Twins in healthcare, noting their properties. It also emphasizes the Blockchain, Smart Contracts and cryptographic notions.

3.1 Multi-receiver Identity-Based Signcryption

A multi-receiver identity-based encryption scheme (mIBSC) comprises four algorithms: Setup, Extract, Signcrypt, and Designcrypt, which are described as follows:

1. Setup(λ, N) $\rightarrow$ ($params$, MSK): The Setup algorithm takes a security parameter λ and N maximal size of the set of receivers for one encryption as input and provides a master secret key MSK and a set of public parameters $params$ as the outputs.
2. Extract$(MSK, ID_i) \rightarrow SK_{ID_i}$: The Extract algorithm takes a master secret key, MSK and an identity, ID_i as input and provides the secret key SK_{ID_i} as an output.
3. Signcrypt$(m, S, ID_{Sender}, SK_{ID_{Sender}}) \rightarrow \sigma$. The signcrypt algorithm takes in message m, the sender's identity ID_{Sender} and the sender's secret key $SK_{ID_{Sender}}$ and a set of identities of recipients $S = \{ID_1, \ldots, ID_t\}$, with $s \leq N$, and returns signcryption σ of m from $SK_{ID_{Sender}}$. The broadcast message to users in S is made up of (S, ID_{Sender}, C_T).
4. Designcrypt$(\sigma, S, ID_{Sender}, ID_i, SK_{ID_i}) \rightarrow m$: The Designcrypt algorithm takes in a signcryption σ, a subset $S = \{ID_1, \ldots, ID_t\}$, with $s \leq N$, the sender's identity ID_{Sender}, a receiver's identity ID_i and the associated private key SK_{ID_i}. If $ID_i \in S$, the algorithm returns the message m. Otherwise it returns an error symbol $\perp$.

Note that the public parameters $params$ have been omitted for a concise description of the algorithms in mIBSC scheme. Due to page limitations the confidentiality and unforgeability security models of mIBSC have been omitted. Readers can refer to [25] for the security models.

3.2 Digital Twins

A patient Digital Twin is an evolving data-driven model that presents increasingly detailed approximations of a patient's condition(s). Data from patients' Electronic Medical Records (EMRs) and other relevant data sources can be combined and analyzed to produce a computational model to represent the patient digitally. Thus, analyses of the Digital Twin can facilitate predictions in sensitive areas such as experimental drug interactions [32], performance of tasks, create working models of organs, and study the behavior of physiological systems. The patient's Digital Twin needs properties that facilitate analytics and other services. We describe these properties briefly below:

- **Adaptability**: For a patient Digital Twin, we define adaptability as the capacity to accept and incorporate changes to the Digital Twin so that it can adjust to suit predicted, anticipated, or stochastic changes. The virtual model must accommodate the changes that occur over its lifetime. Critically, the adaptability property provides the basis for other properties as well.
- **Extensibility**: The Digital Twin must be extensible to account for new parameters to be tracked for optimal operation and performance. For a patient's Digital Twin, this is important for the several cycles of health conditions a patient may have over time. Extensibility allows the addition of new modules to enable functionality and capabilities so the Digital Twin can grow.
- **Modularity**: Aspects of the person that require monitoring can be virtualized and updated to provide insights for improved care. The patient Digital Twin can therefore be composed of several distinct but interconnected modules grouped into logical categories. These modules may represent physiological systems, conditions, etc. The modules can include all data relevant to patient care.

- **Connectivity**: Connectivity distinguishes the Digital Twin from other analytic models. Hence, we define connectivity as the capacity to connect to systems, platforms, and services to provide data for operating the physical asset. It may be updated periodically from data sources with changes in predefined categories of data, contexts, and conditions. The availability of new data, bandwidth, etc., can determine the frequency of connectivity.
- **Programmability**: The patient Digital Twin can support experiments by taking data inputs that can be processed to determine desirable outcomes within constrained boundaries and under specific conditions to support optimal health. Thus, a Digital Twin instance can test and adaptively refine treatment until the desired outcome is optimal. Conversely, failure of such experiments has no disadvantage for the patient since the Digital Twin can have multiple instances.
- **Flags**: The Digital Twin can represent a set of distinct conditions and system states that a physical system manifests under specified constraints. The Digital Twin can provide data to adaptively and preemptively manage the patient's condition(s) through simulations. Thus, the twin can receive configurations that respond to each medical condition's thresholds.

3.3 Blockchain

The blockchain is a linked-list data structure and a consensus protocol initially designed to prevent double-spending in Bitcoin. Each block b in the blockchain β is a container that holds transaction data. The blockchain maintains an extending list of transactions such that each node contains copies of transactions accepted by the network. Transactions in the blockchain are immutable and pseudonymous, and users may generate a new address for each transaction to achieve credible anonymity on the network. Nodes collaborate to confer transaction validity through a consensus mechanism, so that a single coherent version of history is maintained as the basis for further action. This blockchain property provides behavioral data for developing the patient's Digital Twin. Fig 2 depicts a visual representation of the blockchain showing how transactions are linked. We base our system on the blockchain to account for the following:

- **Preemptive Assumptions on User Behavior**: The patient Digital Twin is a data-sharing agent that provides insights on specific aspects of the patient's health. A requester may exhibit behavior that deviates from care requirements, so capturing all requests/responses is crucial to account for connections between healthcare goals and outcomes. Thus, we capture instances of the patient Digital Twin for offline storage while proof of their existence is stored on the blockchain. The timestamps of Digital Twin instances and blockchain data are essential in preemptively constructing a timeline for the sequence of actions that definitively establish cause and effect.
- **Consistent View of Transactions**: For specialized care, patients' mobility among several hospitals makes healthcare a collaborative venture. However, hospitals do not update one another on patients' progress for obvious regulatory, competitive, and economic reasons. Thus, while a complete, consistent view of a patient's medical history is beneficial, it may be unavailable. Using a patient Digital Twin instance for each hospital, the patient can maintain a master Digital Twin that synchronizes with the other instances after validation.
- **Immutability of Records**: Since a complete medical history is critical to the treatment, the blockchain can be used to create and sustain a distributed, immutable ledger of Digital Twin instances for the patient. This guarantees access to health records for caregivers in multiple institutions while ensuring that appending data to patient Digital Twin instances cannot be

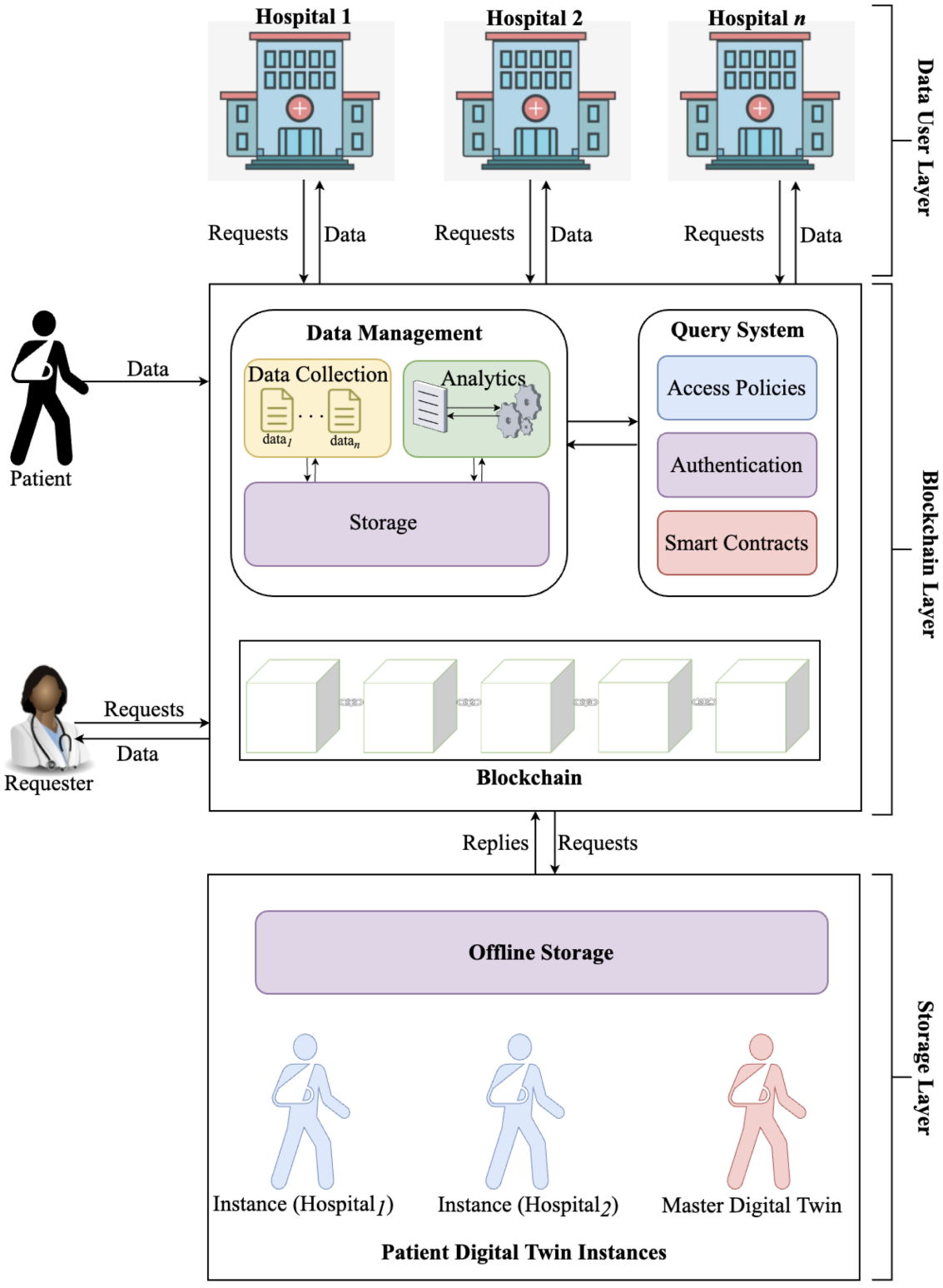

Fig 2. A visual representation of transactions on the blockchain.

https://doi.org/10.1371/journal.pone.0286120.g002

performed without the proper permissions. Thus, timestamped updates to Digital Twin instances and their hashes combine to provide greater security.

3.4 Smart contracts

We include the blockchain in our research to fully take advantage of the Smart Contract functionality. A *smart contract* is a script stored and executed on the blockchain by a connected node after meeting specific contract conditions. By encoding desirable actions as respondent scripts without specifying which node can perform them, we can ensure required interactions are censorship-resistant. It is critical to automate the predictable aspects of Digital Twin operations like updates and limit manual interactions by users other than the patient and approved caregivers. Smart contracts securely decentralize the Digital Twin update process by conceptualizing the patient as a set of interacting scripts, as shown in Fig 3. While smart contracts are not the only way to secure updates to the Digital Twin, they rely on other blockchain properties to offer extra layers of security through data provenance [33]. In this research, we used the Ethereum blockchain because of its global user base and support for smart contracts.

4 System overview

This section presents an overview of the proposed blockchain-secure patient Digital Twin system using smart contracts. Fig 4 shows the overall system architecture. The proposed system has several entities, including the data owner (patient), data users (hospitals), and the system itself, which includes data management, query system, and blockchain network. These entities

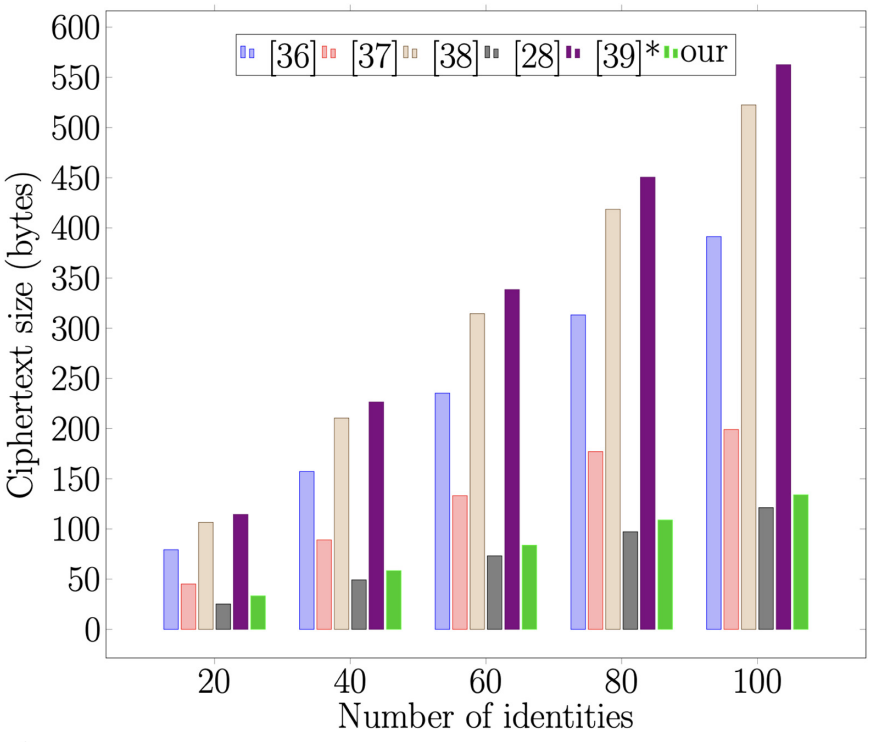

Fig 3. A conceptual overview of the Digital Twin as a construct of smart contracts.

https://doi.org/10.1371/journal.pone.0286120.g003

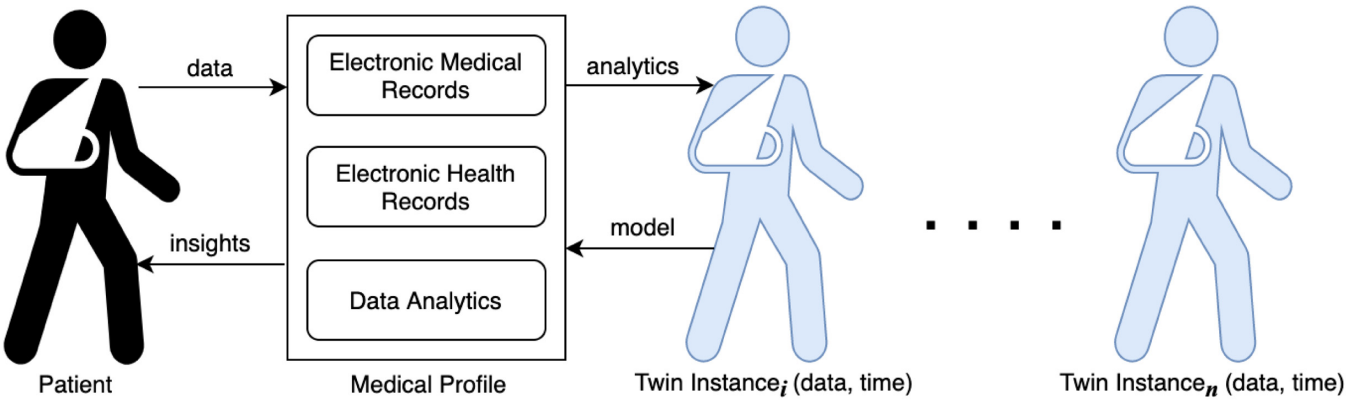

Fig 4. Overall system architecture for patient Digital Twin.

https://doi.org/10.1371/journal.pone.0286120.g004

work together to ensure seamless interactions and secure data sharing among the components of the system. Below is a brief description of the system entities and their functions:

1. **Data owner**:The patient is the owner of the data obtained from sensors, hospital records, and other health records required to create their digital twin. However, the franchise of the data is given to the hospital to maintain accurate health records to secure the wellness of the patient without any security breaches. Therefore, the hospital is the custodian of the data.
2. **Hospitals**: Hospitals play a crucial role in creating complete medical information for the patient to generate master records, which are accurate, fresh, computed, and sound to create a digital twin for the patient. Nurses and doctors who deal directly with the patient's digital twin for good health provision are considered trustworthy to execute their roles without being an adversary for data breaches. The system ensures that encrypted data used in creating the patient digital twin is accessible only to those authorized in the hospital to avoid sensitive information falling into the wrong hands.
3. **Patient**: In the context of this research, a patient is defined as a human entity who seeks healthcare services from a hospital and is a primary data contributor in the healthcare system. The healthcare services that the patient receives require data sharing transactions with other entities within the hospital or outside of it. Hence, the patient's medical record is essential for proper care and can also be shared with other healthcare providers as necessary upon authorised request.
4. **Query System**: The Query System has three components and processes users' requests for access to the patient Digital Twin. The first is the Authentication module which verifies the source and destination of requests before they can be processed. It connects to an Access Policies module which is the second component to check for specific permissions patients define when they first register in the system as users. The third is the Smart Contracts module which executes the transaction of data access after the first two modules have successfully processed a user's request.
5. **Data Management**: This component presents an interface for participating hospitals to provide data on patients. It receives patient data from the hospitals and assigns it to the respective Digital Twin after performing preliminary analytics to check for new content for updating the patient Digital Twin. It has three modules: Data Collection, Analytics, and

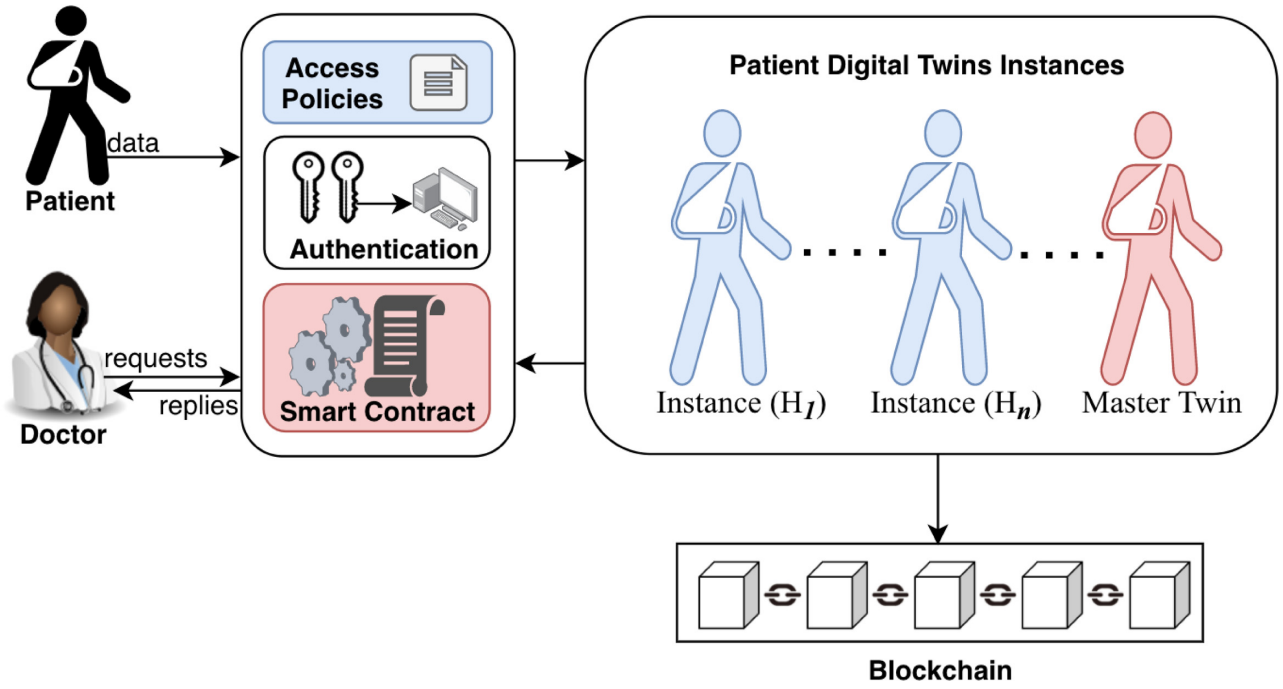

Fig 5. A visual representation of patient Digital Twin instances on the blockchain.

https://doi.org/10.1371/journal.pone.0286120.g005

Storage modules. The Storage is partitioned into two distinct areas of administration: online Storage for operational data and offline Storage for data at rest, such as inactive Digital Twin instances.

6. **Blockchain**: The blockchain network receives and stores completed transactions from network nodes. The data from complete transactions is first prepared into discrete blocks containing transaction details of import to patient care. In this study, we define the blockchain as a decentralized and distributed network of participating hospitals that collectively maintain a tamper-proof and transparent record of longitudinal patient data using consensus mechanisms, cryptographic algorithms, and smart contracts. The patient's latest transaction hash is included in the current block, along with records of queries, access requests, and hashes of patient Digital Twin instances as shown in Fig 5. The blockchain network's version of transactions takes precedence over any single institution's records, ensuring transparency and accountability.

5 System design

In this section, we will present a thorough description of the proposed scheme's design and provide an illustrative scenario of its application.

5.1 Multi-receiver Identity-Based Signcryption(mIBSC)

5.1.1 ***Setup*****(λ, *N*) → (*params*, *MSK*).** The scheme's security parameter is λ, and the maximum size of the collection of receivers is N. $\mathbb{G}_1, \mathbb{G}_2$ are two prime groups of order p such that $|p| = \lambda$. $g \in \mathbb{G}_1$ and $h \in \mathbb{G}_2$ such that a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Lets call the number of

bits required to indicate an identity and a message n_0 and n_1, respectively. Three hash functions are used: $\mathcal{H}_1 : \{0,1\}^{n_0} \rightarrow \mathbb{Z}_p^*, \mathcal{H}_2 : \{0,1\}^{n_1} \times \mathbb{G}_2 \rightarrow \mathbb{Z}_p^*$, and $\mathcal{H}_3 : \mathbb{G}_2 \rightarrow \{0,1\}^{(n_1)+|\mathbb{G}_2|}$. The PKG selects $\gamma \xleftarrow{\$} \mathbb{Z}_p^*$ and calculates $w = g^{\gamma}$ and $u = e(g, h)$. The public parameters are as follows:

$$params \leftarrow (w, u, h, h^{\gamma}, \ldots, h^{\gamma^N})$$

The Master Secret Key is

$$MSK = (g, \gamma).$$

5.1.2 Extract$(ID_i, MSK) \rightarrow SK_{ID_i}$. The PKG runs the Extract algorithm with the input of the user identity ID_i and master secret key $MSK = (g, \gamma)$. Upon successful validation of the ID_i, the PKG computes the secret key as $SK_{ID_i} = g^{\left(\frac{1}{\mathcal{H}_1(ID_i)+\gamma}\right)}$. As a patient medical data is tailored into a Digital Twin to predict how a patient would respond to a given medication, the health models and data must be stored chronologically. Hence, a doctor may be confident that the patient digital twin holds accurate data and that all computational results on the patient digital twin are correct. This permits the doctor to see how a patient digital twin responds to a set of data input over time. Before outsourcing medical data to a cloud server, the hospital employs a smart contract to establish blockchain proof to achieve immutable sequential order.

5.1.3 Signcryption. Suppose a hospital with an identity ID_{Sender}, and a private key $SK_{sender} = g^{\left(\frac{1}{\mathcal{H}_1(ID_{Sender})+\gamma}\right)}$ wants to signcrypt a patient's health data and a Digital Twin which are denoted here as m such that t healthcare providers of the identities $ID_1, \ldots, ID_t$ can access the data, it performs the following:

- Select $k \xleftarrow{\$} \mathbb{Z}_p^*, \leftarrow \{0,1\}^n$.
- Compute the following:
  - $C_1 = w^{-k}$
  - $C_2 = h^{k \cdot \prod_{i=1}^{S}(\gamma + \mathcal{H}_1(ID_i))}$
  - $C_3 = m \cdot u^k$.
  - $f = \mathcal{H}_2(m, C_1, C_2, C_3)$
  - $v = SK_{sender}^{-kf}$
- Output Signcryption$(m, S, ID_{Sender}, SK_{ID_{Sender}})$ of m as $\sigma = (C_1, C_2, C_3, v, \mathcal{L})$, where $\mathcal{L}$ is the list of the recipients who can be authorized to designcrypt σ.

Here, we provide the details on how a patient digital twin is created. First, in Algorithm 1, a smart contract is deployed by the private key generator. It has to authorize a hospital before it uses Algorithm 2 to create an instance of the patient digital twin. Patients provide data to hospital data management platforms, as shown in the overall system architecture in Fig 4. To create the digital twin, one first provides a list of data sources that can later be updated. Ideally, these are hospital databases that host detailed patient data and online storage platforms for Personal Health Records from wearable sensors and other devices. A patient may have a digital twin for each unique condition such as disease progression, an organ, the whole body, etc.

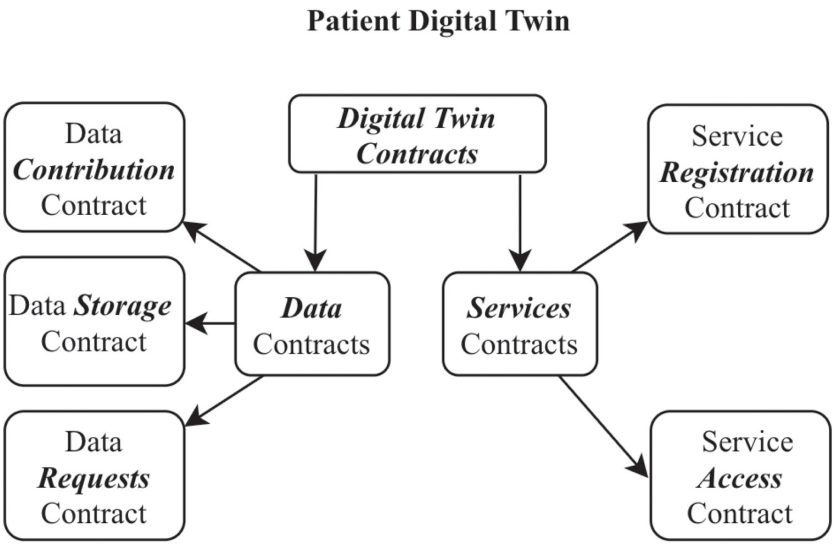

Fig 6. A visual representation of patient Digital Twin data request and response.

https://doi.org/10.1371/journal.pone.0286120.g006

Thus, for each patient, doctors can access multiple digital twin instances, as shown in Fig 6. Formally, a digital twin instance T_i, as proposed in this research, is a tuple of data sources, $\sigma = [\sigma_1, \sigma_2, \ldots, \sigma_n]$, and identity of hospital ID_H, patient ID_P and ciphertext auxiliary v which are encoded into smart contract as $v = [v_1, v_2, \ldots, v_n]$ in Algorithm 2. The smart contract execution generates a cryptographic hash of the twin instance, h_i, Merkel root, mk_i, block number, b_i, and a timestamp, t_s, to facilitate proper sequencing of the digital twin instances. The digital twin instance T_i is represented as shown below.

$$T_i = \{\sigma_i, h_i, mk_i, b_i, t_s\}. \tag{1}$$

After being generated, the patient digital twin can be updated continuously to provide the details required for effective care. Hence, for this research, the primary smart contracts included, such as Algorithms 1 and 2, facilitate patient digital twin updates, access to health services, and provenance of the patient digital twin data. Finally, the hospital sends the digital twin instance T_i to the cloud server for sequential tracking of the various healthcare centers the patient visits. The EmitNotification alerts the hospitals about the new record update and alerts the hospital about the current digital twin instance.

Algorithm 1: AH: Authorized Hospitals

```
Data: Identity of hospital (ID_H), Address (Addr)
Result: True/False
1 struct {
2   _ID_H,A ddr;
3 } T;
4 mapping(ID_H ⇒ T) AuthorizedHospitalList;
5 AuthorizedHospitalList[ID_H] ·_ID_H ← True;
6 AuthorizedHospitalList[ID_H]·_Addr ← True;
7 EmitNotification(ID_H,Addr, msg.sender) /* The EmitNotification trig-
  ger event on the blockchain which hospital ID_p can listen to get
  informed        */
```

5.1.4 Unsigncryption$(S, \sigma, ID_{sender}, SK_{ID_i}, ID_i, params)$**.** To recover the message m from the ciphertext σ, a data user with the private key $SK_{ID_i} = g^{\left(\frac{1}{\mathcal{H}_1(ID_i)+\gamma}\right)}$ and identity ID_i ($ID_i \in S$) performs the following:

1. Compute
   $R = (e(C_1, h^{p_{i,S}(\gamma)}) \cdot e(SK_{ID_i}, C_2))^{\frac{1}{\prod_{j=1,j\neq 1}^{S} \mathcal{H}_1 ID_j}}$ with
   $p_{i,S}(\gamma) = \frac{1}{\gamma} \cdot (\prod_{j=1,j\neq i}^{S}(\gamma + \mathcal{H}_1(ID_j)) - \prod_{j=1,j\neq i}^{S} \mathcal{H}_1(ID_j))$.
2. Recover the message as $m = C_3/R$ and compute $f = \mathcal{H}_2(m, C_1, C_2, C_3)$
3. Accept the message m if $e(v, h^{\gamma} h^{\mathcal{H}_1(ID_{sender})}) \cdot R^f == 1$; otherwise output the error symbol $\perp$.

5.2 Correctness

Considering σ is well formed ciphertext for S:

$$
\begin{aligned}
R' &= e(C_1, h^{p_{i,S}(\gamma)}) \cdot e(SK_{ID_i}, C_2) \\
&= e(g^{-k\cdot\gamma}, h^{p_{i,S}(\gamma)}) \cdot e\left(g^{\frac{1}{\mathcal{H}_1(ID_i)+\gamma}}, h^{k\cdot\prod_{j=1}^{S}(\gamma+\mathcal{H}(ID_j))}\right) \\
&= e(g,h)^{-k\cdot(\prod_{j=1,j\neq i}^{S}(\gamma+\mathcal{H}_1(ID_j)) - \prod_{j=1,j\neq i}^{S}\mathcal{H}_1(ID_j))} \cdot \\
&\quad e(g,h)^{k\cdot\prod_{j=1,j\neq i}^{s}(\gamma+\mathcal{H}(ID_j))} \\
&= e(g,h)^{k\cdot\prod_{j=1,j\neq i}^{S}\mathcal{H}_1(ID_j)} \\
&= R^{\prod_{j=1,j\neq i}^{S}\mathcal{H}(ID_j)} \\
&\text{Thus } R'^{\frac{1}{prod_{j=1,j\neq i}^{S}\mathcal{H}_1(ID_j)}} = R = e(g,h)^k
\end{aligned}
$$

Then, the correctness of signature is performed as:

$$
\begin{aligned}
& e(v, h^{\gamma} h^{\mathcal{H}_1(ID_{sender})}) \cdot R^f == 1 \\
& e\left(g^{\left(\frac{1}{\mathcal{H}_1(sender)+\gamma}\right)^{-kf}}, h^{\gamma+\mathcal{H}_1(ID_{sender})}\right) \cdot e(g,h)^{kf} == 1 \\
& (g,h)^{\left(\frac{\mathcal{H}_1(ID_{sender})+\gamma}{H_1(ID_{sender}+\gamma}\right)^{-kf}} \cdot e(g,h)^{kf} == 1 \\
& e(g,h)^{-kf+kf} == 1
\end{aligned}
$$

After successful unsigncryption of the ciphertext which is part of the digital twin data T_i recovered from the cloud server, the hospital, decryptor uses the block number b_i to confirm that the twin instance h_i the Merkel root mk_i and all other details of the digital twin are true on the blockchain. Note that the Merkel root guarantees the sequence of the digital twin.

Algorithm 2: PDTC: Patient Digital Twin Creation

```
Data: ciphertext auxiliary v, identity of hospital ID_H, patient ID_P
1 struct {
2   _ID_H, _ID_P, _v;
3 } T;
```

```
mapping(address ⇒ T) DataTwin;
AH ah = AH();
  /* Algorithm 1 is called here          */
if ah· AuthorizedHospitalList[ID_H] and ah· AuthorizedAddressList[msg.
  sender] then
   DataTwin[msg.sender]·_ID_H ← ID_H;
   DataTwin[msg.sender]·_ID_P ← ID_P;
   DataTwin[msg.sender]·_v ← v;
    EmitNotification(ID_H, ID_S, P, msg.sender)
end
  /* The EmitNotification alerts the hospitals about the new record
update */
```

5.3 Application scenarios

The proposed scheme for Blockchain-secure Patient Digital Twin in Healthcare using Smart Contracts can be applied in various domains of healthcare, such as chronic disease management, mental health disorders, patient monitoring, and personalized healthcare. The scheme can help improve the management of these health conditions by securely storing and accessing patient data on the blockchain, while also ensuring data confidentiality, integrity, and privacy through smart contract-based access control and cryptographic techniques.

One of the potential application of the proposed scheme is in managing mental health disorders. A patient with a mental health disorder can use wearable devices to collect data on their mood, sleep patterns, medication adherence, and other health metrics. The data can be securely stored on the cloud repository using Multi-receiver Identity-Based Signcryption (mIBSC) cryptographic technique for data confidentiality and integrity. The data is hashed on the blockchain for secure offline storage and protection of sensitive health information from unauthorized access.

The patient's digital twin (virtual model that captures the essence of a patient's medical conditions and interventions, based on the data collected from various sources, such as electronic medical records (EMR) and personal health records (PHR) from wearable devices) would contain a timestamped list of their medical conditions and corrective interventions, including information on medications, treatments, and therapy sessions. The patient digital twin could be used to monitor the patient's progress over time, identify trends and patterns in their health data, and provide personalized recommendations for managing their mental health disorder.

For example, if the patient's mood is consistently low at certain times of day, the digital twin could suggest adjustments to their medication regimen or therapy sessions. If the patient's sleep patterns change, the digital twin could track the impact on their mood and adjust recommendations accordingly. Smart contracts can provide access control to the patient digital twin, enabling the patient to choose who can view and update their health information. The system could also monitor medication adherence and identify potential adverse drug interactions.

In summary, the proposed scheme can be a powerful tool for improving the management of healthcare and delivering personalized, data-driven care to patients. The use of mIBSC and smart contract-based access control would help ensure the privacy, security, and integrity of the patient's health data, while also enabling secure offline data storage.

6 Security proof

Using the Gap Diffie-Hellman Exponent (GDDHE) assumption of [34], we demonstrate the IND-sID-CPA security of our system. We begin by defining the intermediate decisional problem as follows.

Definition 1 *((f,g,F)-GDDHE). Let* $\mathcal{B} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(,))$ *denotes a bilinear map group system and let f and g represent two coprime polynomials with distinct pairwise roots with respective orders t and n. Let* g_0 *denotes a generator of* $\mathbb{G}_1$ *and* h_0 *be a generator of* $\mathbb{G}_2$*. Solving the (f,g,F)-GDDHE problem consists*:

$$g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{t-1}}, g_0^{\gamma \cdot f(\gamma)}, g_0^{k \cdot \gamma \cdot f(\gamma)},$$
$$h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{2n}}, h_0^{k \cdot g(\gamma)},$$

The adversary $\mathcal{A}$ *decides whether* $T \in e(g_0, h_0)^{k \cdot f(\gamma)}$ *or T is a random element in* $\mathbb{G}_T$.

Definition 2 *(l-SDHP Problem) The l-Strong Diffie– Hellman problem (l—SDHP) in the group G consists of, given* $g_0, g_0\gamma, \ldots, g_0^{\gamma l}$*, finding a pair* $\left(c, g_0^{\frac{1}{c+\gamma}}\right)$ *with* $c \in \mathbb{Z}_p^*$ [18]

We denote by $Adv_{\mathcal{A}}^{l-SDHP}$ the advantage of $\mathcal{A}$ in solving the (l—SDHP) in $\mathbb{G}$ and set $Adv_{\mathcal{A}}^{l-SDHP} = Pr\left[\mathcal{A}(g_0, g_0\gamma, \ldots, g_0^{\gamma l}) = \left(c, g_0^{\frac{1}{c+\gamma}}\right)\right]$, where $l, c \in \mathbb{Z}_p^*$. The l—SDHP assumption is that, for any probabilistic polynomial time algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{l-SDHP}$ is negligible.

6.1 Confidentiality

Let $Adv^{gddhe}(f, g, F, \mathcal{A})$ denotes the advantage of $\mathcal{A}$ in distinguishing the distributions (i.e., $T \in_R \mathbb{G}$ or $T \in (g_0, h_0)^{k \cdot f(\gamma)}$, where $\in_R$ denotes random selection of an element in $\mathbb{G}$).

Corollary 0.1 *For any probabilistic algorithm* $\mathcal{A}$ *that sends at most q queries to the oracle, the adversary* $\mathcal{A}$ *has*:

$$Adv^{gddhe}(f, g, F) \leq \frac{(q + 2(n + t + 4) + 2)^2 \cdot d}{2p}$$

where, $d = 2 \cdot max(n, t + 1)$, $t \in_R Z_q$*, and n is the total number of identities.*

Theorem 1 *For any n, t we have* $Adv_{mIBSC}^{\text{IND}-\text{sID}-\text{CPA}} \leq 2 \cdot Adv^{gddhe}(f, g, F)$

Algorithm $\mathcal{C}$ is provided with the input $\mathcal{B} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e(,))$, and a (f,g,F)-GDDHE instance in $\mathcal{B}$ (as described in Definition 1). Hence, we have f and g two coprime polynomials with pairwise distinct roots, of respective orders t and n, and $\mathcal{C}$ is given

$$g_0, g_0^{\gamma}, \ldots, g_0^{\gamma^{t-1}}, g_0^{\gamma \cdot f(\gamma)}, g_0^{k \cdot \gamma \cdot f(\gamma)},$$
$$h_0, h_0^{\gamma}, \ldots, h_0^{\gamma^{2n}}, h_0^{k \cdot g(\gamma)},$$

and $T \in \mathbb{G}_T$, decides whether $T \in e(g_0, h_0)^{k \cdot f(\gamma)}$ or T is a random element in $\mathbb{G}_T$. We indicate that f and g are unitary polynomials for clarity, but this is not a requirement.

6.2 Notations

- $f(X) = \prod_{i=1}^{t}(X + x_i), g(X) = \prod_{i=t+1}^{t+n}(X + x_i)$
- $f_i(x) = \frac{f(x)}{x+x_i}$ for $i \in [1, t]$, which is a polynomial of degree $t - 1$
- $g_i(x) = \frac{g(x)}{x+x_i}$ for $i \in [t + 1, t + n]$, which is a polynomial of degree $n - 1$

1. **Init**: The adversary $\mathcal{A}$ commits a set $S^* = ID_1^*, \ldots, ID_{t^*}^*$ of identities that it wants to attack (with $t^* \leq n$).

2. **Setup**: To produce the system parameters, $\mathcal{C}$ sets $g = g_0^{f(y)}$ (i.e. without computing it) and sets

$$\begin{aligned} h = &\quad h_0^{\prod_{i=t+s^*+i}^{t+n}(\gamma+x_i)}, w = g_0^{\gamma \cdot f(\gamma)=g^{\gamma}}, \\ v &= e(g_0, h_0)^{f(\gamma)\cdot\prod_{t+s^*+1}^{t+n}(\gamma+x_i)} = e(g, h). \end{aligned}$$

Eventually, $\mathcal{C}$ defines the public parameters as $params = (w, u, h, h^{\gamma}, \ldots, h^{\gamma^N})$. Note that the challenger $\mathcal{C}$ is restricted from accessing the element g. $\mathcal{C}$ runs $\mathcal{A}$ on the system parameters $\mathcal{B}, \mathcal{H}_1, \mathcal{H}_2$ and params. Here, the hash oracles $\mathcal{H}_1, \mathcal{H}_2$ are controlled by $\mathcal{C}$.

3. **Query Phase 1**: At any point in time, the adversary $\mathcal{A}$ can query the following random oracles. To answer the queries, $\mathcal{C}$ maintains two lists $\mathcal{L}_{\mathcal{H}_1}$ and $\mathcal{L}_{\mathcal{H}_2}$.

- $\mathcal{H}_1$ queries: The list $\mathcal{L}_{\mathcal{H}_1}$ contains at the beginning:

$$\{(*, x_i, *)\}_{i=1}^{t}, \{(ID_i, x_i, *)\}_{i=t+1}^{t+s^*}$$

(We select * to represent an empty element in $\mathcal{L}_{\mathcal{H}_1}$. When $\mathcal{A}$ decides to query on identity ID_i,

(a) If ID_i already exists in the list $\mathcal{L}_{\mathcal{H}_1}$, $\mathcal{C}$ answers with x_i.

(b) Else, $\mathcal{C}$ sets $\mathcal{H}_1(ID_i) = x_i$ and completes the list with (ID_i, x_i, *).

- $\mathcal{H}_2$ queries: To respond to this query, $\mathcal{C}$ keeps a list of tuples known as $\mathcal{L}_{\mathcal{H}_2}$ list. Each entry in this tuple is of the form (m, C_1, C_2, C_3). At the beginning of the list, it is empty. To respond to queries, algorithm $\mathcal{C}$ performs the following:

- If the queries on (m, C_1, C_2, C_3) is in the list (m, C_1, C_2, C_3, f), then respond with $f = \mathcal{H}_2(m, C_1, C_2, C_3)$.

  - Else, $\mathcal{C}$ selects a random $f \in \mathbb{Z}_p^*$ and updates $L_{\mathcal{H}_2}$ list with (m, C_1, C_2, C_3, f). $\mathcal{C}$ outputs f to $\mathcal{A}$.

4. **Extraction queries**: The challenger $\mathcal{C}$ runs $\mathcal{O}_{Extract}$ on $ID_i \notin S^*$ and sends the associated private key SK_{ID_i} to the adversary $\mathcal{A}$. To generate the keys,

- If $\mathcal{A}$ has already issued an extraction query on ID_i, $\mathcal{C}$ responds with the associated SK_{ID_i} in the list $\mathcal{L}_{\mathcal{H}_1}$.

- Otherwise, if $\mathcal{A}$ already issued a hash query on ID_i, then $\mathcal{C}$ uses the associated x_i to generate $SK_{ID_i} = g_0^{f_i(\gamma)} = g^{\frac{1}{\gamma+\mathcal{H}_1(ID_i)}}$ and then updates the list $\mathcal{L}_{\mathcal{H}_1}$ with SK_{ID_i} for ID_i.

- Otherwise, $\mathcal{C}$ sets $\mathcal{H}_1(ID_i) = x_i$, generates the associated SK_{ID_i} exactly as stated earlier and completes the list $\mathcal{L}_{\mathcal{H}_1}$ with SK_{ID_i} for ID_i.

5. **Challenge** At some point in time, $\mathcal{C}$ decides that phase 1 is over, challenger $\mathcal{C}$ computes Signcrypt$(m, S^*, ID_{Sender}, SK_{ID_{Sender}}, params) \rightarrow \sigma^*$, where

$$\begin{aligned} C_1 = &\quad g_0^{-k\cdot\gamma\cdot f(\gamma)}, C_2 = h_0^{k\cdot g(\gamma)}, C_3 = m_b \cdot T^{\prod_{i=t+s^*+1}^{t+n} x_i}. \\ &\quad e(g_0^{k\cdot\gamma\cdot f(\gamma)}, h_0^{q^{\gamma}}) \\ f = &\quad \mathcal{H}_2(m_b, C_1, C_2, C_3), v^* = SK_{sender}^{-kf} \end{aligned}$$

Here the challenger $\mathcal{C}$ randomly selects $b \leftarrow 0, 1$ and sets $m = m_b$. $\mathcal{C}$ returns $\sigma^* = (C_1, C_2, C_3^*, v^*)$. with $q(\gamma) = \frac{1}{\gamma}\left(\prod_{i=t+s^*+1}^{t+n}(\gamma + x_i) - \prod_{i=t+s^*+1}^{t+n}(x_i)\right)$. One can verify that

$$\begin{aligned} C_1 &= w^{-k}, \\ C_2 &= h_0^{k\cdot\prod_{i=t+s^*=1}^{t+1}(\gamma+x_i)\cdot\prod_{i=t+1}^{t+s^*}(\gamma+x_i)} \\ &= h^{k\cdot\prod_{i=t+1}^{t+s^*}(\gamma+\mathcal{H}_1(ID_i^*))} \end{aligned}$$

Note that if $T = e(g_0, h_0)^{k\cdot f(y)}$, then $C_3 = m_b \cdot u^k$.

6. **Query Phase 2**: This phase is same as phase 1. The adversary $\mathcal{A}$ continues to issue queries with the restriction that no extraction query is committed on $ID_i \in S^*$.

7. **Guess**: Finally, $\mathcal{A}$ returns a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$. One has

$$\begin{aligned} &Adv^{gddhe}(f, g, F, \mathcal{C}) \\ &= Pr[b' = b|real] - Pr[b' = b|rand] \\ &= \frac{1}{2} \times (Pr[b' = 1|b = 1 \wedge real] - \\ &Pr[b' = 1|b = 0 \wedge real]) \\ &= \frac{1}{2} \times (Pr[b' = 1|b = 1 \wedge rand] - \\ &Pr[b' = 1|b = 0 \wedge rand]) \end{aligned}$$

In the random situation, the distribution of b is independent of the adversary's point of view. $Pr[b' = 1|b = 1 \wedge rand] - Pr[b' = 1|b = 0 \wedge rand]$. All simulations are perfect, the distributions of all variables defined by $\mathcal{C}$ absolutely conform with the semantic security game. Therefore $Adv_{mIBSC}^{\text{IND}-\text{sID}-\text{CPA}}(t, n\mathcal{A}) = Pr[b' = 1|b = 1 \wedge real] - Pr[b' = 1|b = 0 \wedge real]$. Putting it together, yield $Adv^{gddhe}(f, g, F, \mathcal{C}) = \frac{1}{2} \cdot Adv_{mIBSC}^{\text{IND}-\text{sID}-\text{CPA}}(t, n\mathcal{A})$.

6.3 Unforgeability

Assume that EUF-CMA adversary $\mathcal{A}$ making l extraction queries, $q\mathcal{H}i$ queries to random oracles $Hi(i = 1, 2)$ and q_sc signcryption queries, has an advantage $e \leq 10(q_{sc} + 1)(q_{sc} + q_{H_2})/2k$ against the proposed scheme. Then, there is an algorithm R to solve the $(l + N)$–*SDHP* with advantage

$$e' \geq \frac{1}{9}.$$

R provides the input $(h, h^{\gamma}, \ldots, h^{\gamma^{l+N}})$ and aims to find a pair $\left(c, h^{\frac{1}{c+\gamma}}\right)$. In a setup phase, it constructs a generator $G \in \mathbb{G}_1$ such that it knows $l - 1$ pairs $\left(x_i, G^{\frac{1}{x_i+\gamma}}\right)$ for $x_1, \ldots, x_{l-1} \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. The challenger $\mathcal{C}$ performs the following:

- Select $\eta \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ and set $P = h^{\eta}$.
- Select $x_1, \ldots, x_{l-1} \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ such that $f(z) = \prod_{i=1}^{l-1}(z + x_i)$ to get $c_0, c_1, \ldots, c_{l-1} \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ with $f(z) = \sum_{i=0}^{l-1} c_1 z^i$.

- Set elements $H = h^{\sum_{i=0}^{l-1} c_i \gamma^i = h^{f(\gamma)}}$ and $G = H^{\eta} = p^{f(\gamma)}$.
- Compute $h^{\sum_{i=1}^{l} c_{l-1}\gamma^i} = H^{\gamma}, H^{\gamma^2}, \ldots, H^{\gamma^N}$ and make $\langle G^{\gamma}, H^{\gamma}, H^{\gamma^2}, \ldots, H^{\gamma^N}, e(G,H)\rangle$ public.
- Let $1 \leq i \leq l-1$ and expand $f_i(z) = \frac{f(z)}{(z+x_i)} = \sum_{i=0}^{l-2} d_i z^i$ and $p^{f_i(\gamma)} = G^{\frac{1}{x_i+\gamma}}$.

$\mathcal{A}$ gives $\mathcal{C}$ the target user identity ID_{ℓ}^{*} on which $\mathcal{A}$ wants to forge a signature. $\mathcal{C}$ then prepares to respond to $\mathcal{A}$'s queries throughout the game. It starts by setting the counter i to 1. We will assume that $\mathcal{H}_1$ queries are distinct for the sake of simplicity, and that any query involving an identity ID_i is preceded by the random oracle query $\mathcal{H}_1(ID_i)$.

- $\mathcal{H}_1$ **queries**: On the input of the identity ID_i by $\mathcal{A}$, $\mathcal{C}$ returns a random $x_{\ell} \overset{\$}{\leftarrow} \mathbb{Z}_p^*$ if $ID_i = ID_{\ell}^{*}$. Else, $\mathcal{C}$ responds x_i and increases i. $\mathcal{C}$ stores (ID_i, x_i) in a list $\mathcal{L}_{\mathcal{H}_1}$. Note $\mathcal{H}_2$ query is same as in the confidentiality proof, so it is omitted here.
- **Key generation queries on** $ID_i \neq ID_{\ell}^{*}$: $\mathcal{C}$ retrieves the matching pair (ID_i, x_i) from $\mathcal{L}_{\mathcal{H}_1}$ and outputs the previously computed $G^{\frac{1}{\gamma+x_i}}$ Note: No extraction query on ID_{ℓ}^{*} can be executed.
- **Forgery**: Signcryption query on $(m, ID_{\mathcal{A}}, ID_1, ID2, \ldots, ID_n)$: If $ID_{\mathcal{A}} \neq ID_{\ell}^{*}$, proceeds normally as in the Signcrypt algorithm. Otherwise, $\mathcal{C}$ performs the following:
  - Select $k \overset{\$}{\leftarrow} \mathbb{Z}_p^*$.
  - Compute the following:
    - $C_1^* = w^{(\gamma+x_{\mathcal{A}})k}$
    - $C_2^* = H^{(\gamma+x_{\mathcal{A}})k \cdot \prod_{i=1}^{n}(x_i+\gamma)}$
    - $C_3^* = m \cdot u^k$.
    - $f^* = \mathcal{H}_2(m, C_1, C_2, C_3)$
    - $v^* = G^{\frac{1}{(\gamma+x_{\mathcal{A}})-kf}}$
  - Add the elements $(m, C_1^*, C_2^*, C_3^*, f^*)$ to $\mathcal{L}_{\mathcal{H}_2}$ list.
  - Output signcryption of m as $\langle C_1^*, C_2^*, C_3^*, v^*, \mathcal{L}\rangle$, where $\mathcal{L}$ is the list of recipients who are authorized to designcrypt σ^*.
- **Unsigncryption** $(S, \sigma^*, ID_{\ell}^{*}, SK_{ID_i}, ID_i, params)$: $\mathcal{C}$ looks up $\mathcal{L}_{H_2}$ for an entry of the form $(m, C_1^*, C_2^*, C_3^*, f^*)$ and checks whether it satisfies the following condition:

$$e\left(G^{\frac{1}{(\gamma+x_{\mathcal{A}})-kf}}, H^{\gamma} H^{\mathcal{H}_1(ID_{\ell}^{*})}\right) \cdot (G,H)^{kf} \overset{?}{=} 1$$

$$e(G,H)^{\left(\frac{x_{\mathcal{A}}+\gamma}{H_1(ID_{\ell}^{*})+\gamma}\right)-kf} \cdot e(G,H)^{kf} \overset{?}{=} 1$$

The case in which $\mathcal{A}$ can generate a valid ciphertext is by correctly guessing the hash value $x_{\mathcal{A}} = \mathcal{H}_1(ID_{\ell}^{*})$ without querying on (ID_{ℓ}^{*}). However, this event occurs only with a negligible probability of $\frac{1}{2^{\kappa}}$.

Note that, with the forking lemma, $\mathcal{A}$ does not perform key generation queries on $ID_i \neq ID_{\ell}^{*}$. Based on the theory of irreflexivity, R can generate the message-signature from σ^* with the private key $sk_{ID_{\ell}}$. Since identity-less chosen message attack is possible with a forking

lemma [35], we unify the sender's message m and identity $\mathcal{A}_\ell$ as a fake message $(\mathcal{A}_\ell, m)$. Supposing $\mathcal{A}$ is an effective forger, then there exists a very powerful algorithm $\mathcal{A}'$ which can produce a pair of signed messages $((\mathcal{A}_\ell, f^*, k^*), v^*)$ and $((\mathcal{A}_\ell, f, k), v)$, where $f \neq f^*$ under the same commitment. $\hat{C}$ interacts with $\mathcal{A}'$and $\mathcal{A}$ to solve the ECDL problem as follows:

1. Based on the forking lemma in [35], by executing $\mathcal{A}$', $\hat{C}$ can derive two distinct equations from the signatures $((ID_\ell, m, f, k), v)$ and $((ID_\ell^*, m, f^*, k^*), v^*)$ as:

$$e\left(G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-kf}}, H^{\gamma}H^{\mathcal{H}_1(ID_\ell^*)}\right)\cdot(G,H)^{kf}=1 \tag{2}$$

$$e\left(G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-k^*f^*}}, H^{\gamma}H^{\mathcal{H}_1(ID_\ell^*)}\right)\cdot(G,H)^{k^*f^*}=1 \tag{3}$$

2. Since both Eqs 2 and 3 satisfy the relations:

$$e\left(G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-kf}}, H^{\gamma}H^{\mathcal{H}_1(ID_\ell^*)}\right)\cdot(G,H)^{kf} \tag{4}$$

$$=e\left(G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-k^*f^*}}, H^{\gamma}H^{\mathcal{H}_1(ID_\ell^*)}\right)\cdot(G,H)^{k^*f^*} \tag{5}$$

Then, Set $T^* = v/v^* = G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-kf}}/G^{\frac{1}{(\gamma+x_{\mathcal{A}_\ell})-k^*f^*}} = G^{\frac{1}{ID_\ell^*+\gamma}}$ (Here, $x_{\mathcal{A}_\ell} = H_1(ID_\ell^*)$). From T^*, R first obtains $a_{-1}, \ldots a_{l-2}$ for which $\frac{f(z)}{(z+x_{\mathcal{A}_\ell})} = \frac{a-1}{(z+x_{\mathcal{A}_\ell})} + \sum_{i=0}^{l-2} a_i z^i$ and computes

$$v^* = [T^* \cdot P^{\prod_{i=0}^{l-2} a_i\gamma_i}]^{\frac{1}{a_1}} = P^{\frac{1}{x_\ell+\gamma}}$$

and $\eta^{-1}\cdot v^* = h^{\frac{1}{x_\ell+\gamma}} = h^{\frac{1}{H_1(ID_\ell)+\gamma}}$ since $P = h^\eta$. Eventually, R outputs the $\left(x_\ell, h^{\frac{1}{x_\ell+\gamma}}\right)$ as the solution to (l + N)—SDHP.

As in [22], if $Adv_{\mathcal{A}}^{\text{mIBBSC}} \geq 10(q_{sc}+1)(q_{sc}+q_{H_2})/2^k$, where l extraction queries, q_{H_i} queries to random oracles $H_i(i = 1, 2)$ and q_{sc} signcryption queries are made, then $Adv_R^{(l+N)R-SDHP} \geq 1/9$.

7 Efficiency evaluation

This section evaluates the efficiency of our scheme as it relates to computational and storage overheads, and the deployment of smart contracts.

7.1 Computational overhead

To demonstrate the efficiency of the proposed scheme relative to other schemes, we perform computation analysis with recent broadcast signcryption schemes: [28, 36–39]. The experiment was conducted on a Windows desktop computer with a 2.0GHz Intel Core i7 processor and 8GB 1600 MHz DDR3 RAM. We used Multi-Precision Integer and Rational Arithmetic C Library (MIRACL), a C++ cryptographic library. The execution times are based on the average of 300 trials. The results of the execution are shown in Table 3. In Table 3, we define the related

Table 3. Running times of time-consuming operations.

Operation	Timing (ms)
Elliptic curve group exponentiation ($\bar{E}$)	1.26
Bilinear pairing($\bar{P}$)	14.32
Pairing-based scalar point multiplication (M_1)	4.34
Elliptic curve point multiplication (M_2)	0.98

https://doi.org/10.1371/journal.pone.0286120.t003

symbols to indicate the computational complexity of the operations. However, only the operations in the table are considered in this paper. Other operations, such as addition, subtraction, and hashing, with little or insignificant computational time, are ignored. The theoretical comparison of our proposed scheme and other related works is shown in Table 4. The computation cost benchmarks are shown in Figs 7 and 8. Although the proposed scheme has a high computation cost compared to other related schemes, when we consider pre-computation of the element, the cost of signcryption becomes $3\bar{E}$ while unsigncryption becomes $3\bar{P}$. Hence, the proposed scheme is efficient in communication and computational aspects. The pre-computation becomes applicable when the set of receivers remains the same as in the previous session. Both broadcasters and receivers can reuse the previous information. The difference is significant because the computation operations are reduced to $3\bar{P}$ for unsigncryption on the client side.

7.2 Communication overhead

Additionally, we examine the communication overhead of the proposed scheme and other related schemes. As in [40], we undertake the size of elements $|\mathbb{G}_1| = 1024$ bits, $|\mathbb{G}_2| = 1024$ bits and $|m|$ = 160 bits. The five schemes are compared in Table 4. The benchmark result in Fig 9 demonstrates unequivocally that the proposed scheme achieves the objectives. The prime objective of the proposed scheme is to have the smallest ciphertext size so that the element which is stored on the blockchain will not increase when the attribute size increases.

7.3 Discussion of smart contract deployment and evaluations

We assume the presence of a sensor that can transmit continuous physiological data from the patient to the aggregation platform represented in our research by the Data Management module. Patients' increasing use of wearable sensors validates our assumption in this respect. The Data Management module collects and processes data using the analytics component to sort through received signals to distinguish status data (such as positioning) from care data, such as

Table 4. Comparison of computational cost and communication cost.

Scheme	Signcryption	Unsigncryption	Ciphertext size
[36]	$(3n+1)\bar{E}$	$M_1 + 3\bar{P} + \bar{E}$	$3\lvert\mathbb{G}_1\rvert + n\lvert Z_p^*\rvert + \lvert ID\rvert$
[37]	$(2n+1)M_2$	$4M_2$	$2\lvert\mathbb{G}_1\rvert + (S+2)\lvert Z_p^*\rvert$
[38]	$(4n+2)\bar{E}$	$\bar{E} + 4\bar{P}$	$(2n+3)\lvert\mathbb{G}_1\rvert$
[28]	$(n+1)M_2$	$3M_2$	$2\lvert\mathbb{G}_1\rvert + (n+2)\lvert Z_p^*\rvert$
[39]*	$nM_1 + (n+5)\bar{E}$	$nM_1 + (n+2)\bar{E} + 3\bar{P}$	$3\lvert\mathbb{G}_1\rvert + (n+1)\lvert ID\rvert$
Ours	$M_1 + (3+n)\bar{E}$	$3\bar{P} + nM_1 + n\bar{E}$	$4\lvert\mathbb{G}_1\rvert + \lvert Z_p^*\rvert$

[39]* = Proposal I

https://doi.org/10.1371/journal.pone.0286120.t004

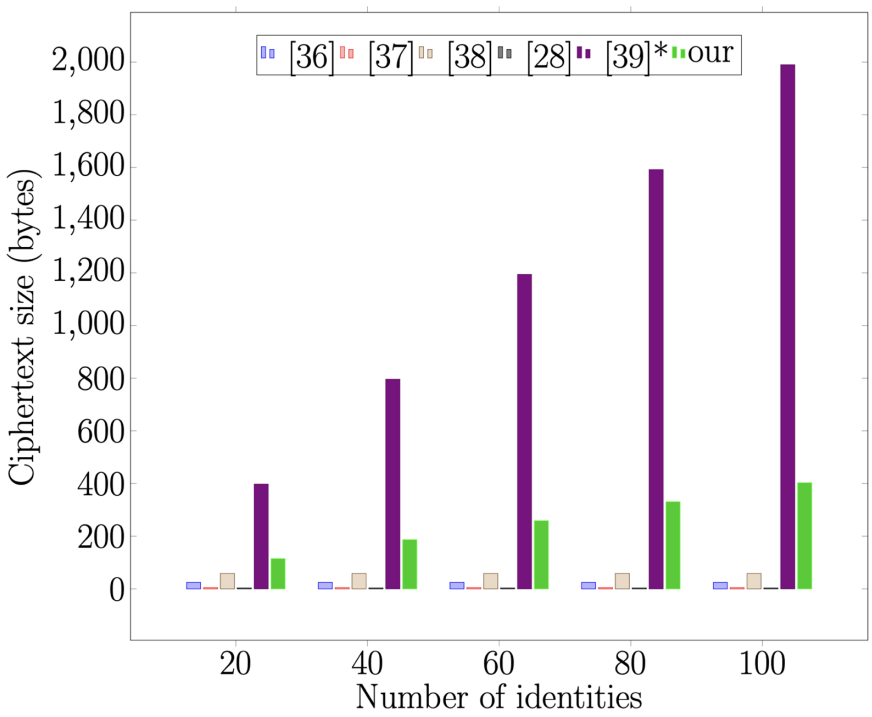

Fig 7. Signcryption.

https://doi.org/10.1371/journal.pone.0286120.g007

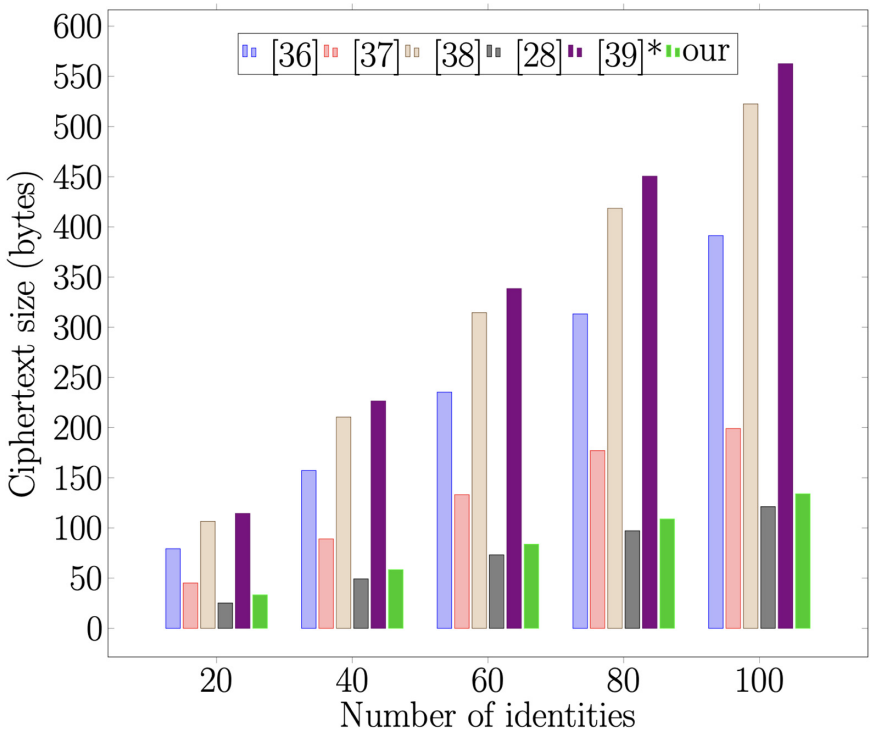

Fig 8. Unsigncryption cost.

https://doi.org/10.1371/journal.pone.0286120.g008

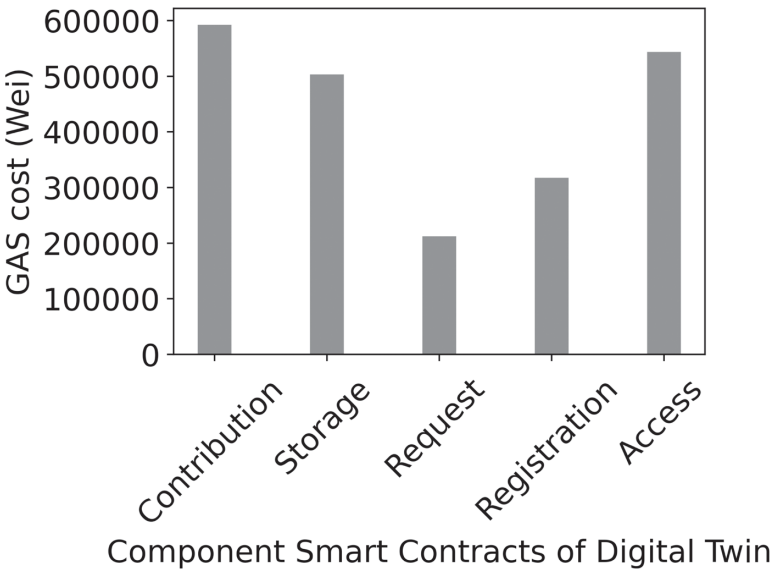

Fig 9. Ciphertext size.

https://doi.org/10.1371/journal.pone.0286120.g009

inputs made by doctors and other caregivers. The output from the analytics module is stored by the connected offline storage till the Query System receives requests for data, or smart contracts are executed to create a patient digital twin instance and to update the master digital twin. The metadata for the transaction, such as hashes, timestamps and commitments, are then prepared into a block and transmitted to the blockchain.

For the experiment, we used the Ropsten Test Environment to test several smart contracts grouped into two categories: Data Contracts and Service Contracts. The Data Contracts handle events relating to data contribution, storage and requests. The Service Contracts deal with services to patients. Each smart contract is invoked using its address on the test Blockchain. Each individual contract was developed using the solidity programming language with the Remix IDE. The appropriate amount of ether was provided by Infura at 4 ETH for all tests needed to run on an Ethereum Decentralized Node with more than 2000 test nodes providing an acceptable degree of consensus. The resources for this experiment were a minimum transaction fee of 0.0002 ETH and a gas rate of 0.27 US dollars per transfer. The computer on which the experiments were performed was an Ubuntu Linux desktop configured with a 1.5 TB Solid State Drive hard drive, 16 GB RAM, and an Intel Core i7 CPU running at 2.67 GHz.

Smart contracts-based patient digital twins can effectively and economically automate patient activities in healthcare considering the current high costs. For example, with the Data Contracts that manage data acquisition and sharing tasks, we measured a total deployment cost of 1308303 Wei on Ethereum, which amounts to about $2.6153, a competitive amount for accessing healthcare. Figs 10 and 11 present the costs of deploying smart contracts in dollars and in Wei while Fig 12 shows the cumulative latency for increasing numbers of user requests. Thus, the aggregate latency for 200 requests in the scheme is 1600 seconds, i.e., 8 seconds per request. The average block confirmation time was approximately 11.7 seconds. The low costs of transactions in both time and monetary terms coupled with our system's provable security make it an effective tool for health data sharing. Even in the unlikely event of a dispute, the immutable records and timestamped transactions provide sufficient input for fault tracing and effective resolution.

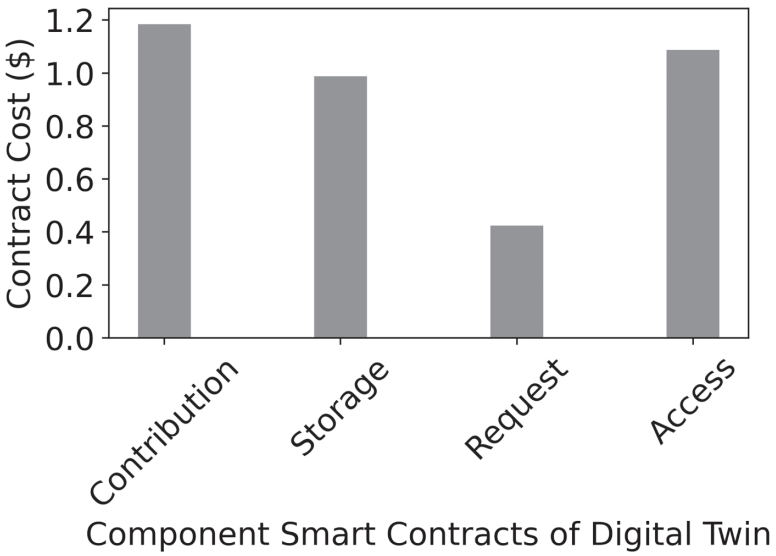

Fig 10. Smart contracts costs in wei.

https://doi.org/10.1371/journal.pone.0286120.g010

Researchers have conducted studies on the use of blockchain in healthcare, focusing on secure data sharing. Most research emphasize the blockchain properties of immutable transactions and distributed storage. None have considered hosting a collection of smart contracts to act as a data-sharing agent on behalf of the patient, as proposed in this research. Hospitals' data sharing requirement for patient care makes our proposed smart contracts-based patient digital twin a necessary addition to healthcare innovation. Thus, we compare our proposed system to blockchain-based health data-sharing papers, each of which has been cited more than 200 times. The comparison is made in Table 5.

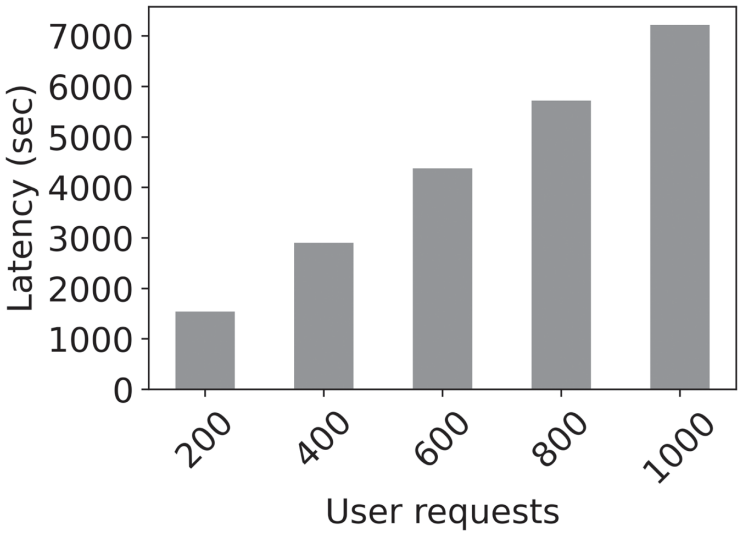

Fig 11. Smart contracts costs in US dollars.

https://doi.org/10.1371/journal.pone.0286120.g011

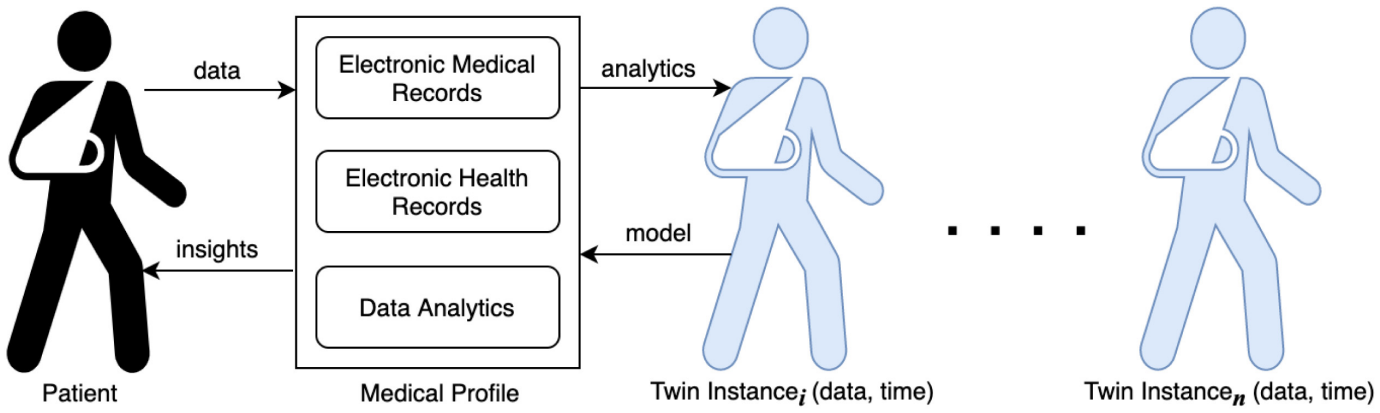

Fig 12. Latency per number of requests in the system.

https://doi.org/10.1371/journal.pone.0286120.g012

Table 5. Comparison of our work with other frameworks for blockchain health data sharing.

Metrics	[36]	[37]	[38]	[28]	[39]	Ours
Blockchain-based	N	N	N	Y	N	Y
Digital Twin-based	N	N	N	N	N	Y
Access Control	Y	Y	Y	Y	Y	Y
Senders and Receivers Known	N	N	N	N	Y	Y
Data Privacy-Preserving	Y	Y	Y	Y	Y	Y

https://doi.org/10.1371/journal.pone.0286120.t005

8 Conclusion

Modern healthcare places unprecedented focus on patient-centered care, which requires secure communication among multiple parties. The process depends on the secure sharing of patient data and can be tedious for those involved. Thus, automation of a data-sharing mechanism with agency such as the patient digital twin can promote efficient interaction between the entities required to administer patient care. This paper proposes a blockchain-secure patient digital twin as a secure construct for personal health data sharing. We use smart contracts on the Ethereum network to ensure that patients have control over their medical records with guaranteed privacy and security. We protect the data and instances of the digital twins generated using proven cryptographic techniques that are also computationally light. We evaluate our research with some experimental results and comparison with other works. Our proposed system can be integrated into existing healthcare platforms using a permissioned blockchain for maximum privacy and security. We hope to extend the research to provide the patient digital twin with greater autonomy.

Supporting information

S1 File.
(ZIP)

S2 File.
(ZIP)

Author Contributions

Conceptualization: Sandro Amofa, Isaac Amankona Obiri.

Data curation: Sandro Amofa, Isaac Amankona Obiri.

Formal analysis: Sandro Amofa, Isaac Amankona Obiri.

Project administration: Qi Xia, Jianbin Gao.

Resources: Jingcong Yang.

Software: Isaac Amankona Obiri, Bonsu Adjei-Arthur.

Supervision: Qi Xia.

Visualization: Hu Xia.

Writing – original draft: Sandro Amofa, Isaac Amankona Obiri.

Writing – review & editing: Sandro Amofa, Isaac Amankona Obiri.

References

1. El Saddik A. Digital twins: The convergence of multimedia technologies. IEEE multimedia. 2018; 25 (2):87–92 https://doi.org/10.1109/MMUL.2018.023121167
2. Moser A, Appl C, Bruning S, Hass VC. Mechanistic mathematical models as a basis for digital twins. In: Digital Twins. Springer; 2020. p. 133–180.
3. Schluse M, Priggemeyer M, Atorf L, Rossmann J. Experimentable digital twins—Streamlining simulation-based systems engineering for industry 4.0. IEEE 627 Transactions on industrial informatics. 2018; 14(4):1722–1731. https://doi.org/10.1109/TII.2018.2804917
4. Popa EO, van Hilten M, Oosterkamp E, Bogaardt MJ. The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks. Life sciences, society and policy. 2021; 17(1):1–25. https://doi.org/10.1186/s40504-021-00113-x PMID: 34218818
5. Eckhart M, Ekelhart A. Towards security-aware virtual environments for digital twins. In: Proceedings of the 4th ACM workshop on cyber-physical system security; 2018. p. 61–72.
6. Amofa S, Sifah EB, Kwame OB, Abla S, Xia Q, Gee JC, et al. A blockchain-based architecture framework for secure sharing of personal health data. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE; 2018. p. 1–6.
7. Xia Q, Gao J, Amofa S. Blockchain Medical Data Sharing. Wireless Blockchain: Principles, Technologies and Applications. 2021; p. 245–268. https://doi.org/10.1002/9781119790839.ch11
8. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information. 2017; 8(2):44. https://doi.org/10.3390/info8020044
9. Sifah EB, Xia Q, Agyekum KOBO, Amofa S, Gao J, Chen R, et al. Chain-based big data access control infrastructure. The Journal of Supercomputing. 2018; 74(10):4945–4964. https://doi.org/10.1007/s11227-018-2308-7
10. Zyskind G, Nathan O, et al. Decentralizing privacy: Using blockchain to protect 647 personal data. In: 2015 IEEE Security and Privacy Workshops. IEEE; 2015. p. 180–184.
11. Ahmadi-Assalemi G, Al-Khateeb H, Maple C, Epiphaniou G, Alhaboby ZA, Alkaabi S, et al. Digital twins for precision healthcare. Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity; Springer Nature Switzerland AG: Cham, Switzerland. 2020; p. 133–158.
12. De Maeyer C, Markopoulos P. Future outlook on the materialisation, expectations and implementation of Digital Twins in healthcare. In: 34th British HCI Conference 34; 2021. p. 180–191.
13. Croatti A, Gabellini M, Montagna S, Ricci A. On the integration of agents and digital twins in healthcare. Journal of Medical Systems. 2020; 44(9): 1–8. https://doi.org/10.1007/s10916-020-01623-5 PMID: 32748066
14. EL Azzaoui A, Kim TW, Loia V, Park JH. Blockchain-based secure digital twin framework for smart healthy city. In: Advanced Multimedia and Ubiquitous Engineering. Springer; 2021. p. 107–113.
15. Akash SS, Ferdous MS. A Blockchain Based System for Healthcare Digital Twin. IEEE Access. 2022;.

16. Nielsen CP, da Silva ER, Yu F. Digital Twins and Blockchain–Proof of Concept. Procedia CIRP. 2020; 93:251–255. https://doi.org/10.1016/j.procir.2020.04.104

17. Altun C, Tavli B. Social internet of digital twins via Distributed Ledger 666 technologies: application of predictive maintenance. In: 2019 27th Telecommunications Forum (TELFOR). IEEE; 2019. p. 1–4.

18. Teng SY, Tous M, Leong WD, How BS, Lam HL, Masa V. Recent advances on industrial data-driven energy savings: Digital twins and infrastructures. Renewable and Sustainable Energy Reviews. 2021; 135:110208. https://doi.org/10.1016/j.rser.2020.110208

19. Yaqoob I, Salah K, Uddin M, Jayaraman R, Omar M, Imran M. Blockchain for digital twins: Recent advances and future research challenges. IEEE Network. 2020; 34(5):290–298. https://doi.org/10.1109/MNET.001.1900661

20. Fiat A, Naor M. Broadcast Encryption; Crypto'93, LNCS 773; 1994.

21. Delerablee C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer; 2007. p. 200–215.

22. Delerablee C, Paillier P, Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: International Conference on Pairing-Based Cryptography. Springer; 2007. p. 39–59.

23. Ren Y, Gu D. Fully CCA2 secure identity based broadcast encryption without random oracles. Information Processing Letters. 2009; 109(11):527–533. https://doi.org/10.1016/j.ipl.2009.01.017

24. Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Annual international cryptology conference. Springer; 2005. p. 258–275.

25. Sharmila Deva Selvi S, Sree Vivek S, Srinivasan R, Pandu Rangan C. An efficient identity-based signcryption scheme for multiple receivers. In: International workshop on security. Springer; 2009. p. 71–88.

26. Zia Ullah Bashir M, Ali R. Correction to: A Multi Recipient Aggregate Signcryption Scheme Based on Elliptic Curve. Wireless Personal Communications. 2021; 120(2):1921–1921. https://doi.org/10.1007/s11277-021-08750-3

27. Fajari MF, Ogi D. Implementation of Efficient Anonymous Certificate-Based Multi-Message and Multi-Receiver Signcryption On Raspberry Pi-Based Internet of Things Monitoring System. In: 2021 International Conference on ICT for Smart Society (ICISS). IEEE; 2021. p. 1–5.

28. Yang X, Li X, Li T, Wang X, Wang C, Li B. Efficient and anonymous multi-message and multi-receiver electronic health records sharing scheme without secure channel based on blockchain. Transactions on Emerging Telecommunications Technologies. 2021; 32(12):e4371. https://doi.org/10.1002/ett.4371

29. Hasan HR, Salah K, Jayaraman R, Omar M, Yaqoob I, Pesic S, et al. A blockchain-based approach for the creation of digital twins. IEEE Access. 2020; 8:34113–34126. https://doi.org/10.1109/ACCESS.2020.2974810

30. Putz B, Dietz M, Empl P, Pernul G. Ethertwin: Blockchain-based secure digital twin information management. Information Processing & Management. 2021; 58(1):102425. https://doi.org/10.1016/j.ipm.2020.102425

31. Amofa S, Gao J, Asante-Mensah MG, Haruna CR, Qi X. Blockchain-Based Patient-to-Patient Health Data Sharing. In: Frontiers in Cyber Security: 5th International Conference, FCS 2022, Kumasi, Ghana, December 13–15, 2022, Proceedings. Springer; 2022. p. 198–210.

32. Agyemang B, Wu WP, Kpiebaareh MY, Lei Z, Nanor E, Chen L. Multi-view self-attention for interpretable drug–target interaction prediction. Journal of Biomedical Informatics. 2020; 110:103547. https://doi.org/10.1016/j.jbi.2020.103547 PMID: 32860883

33. Kusi GA, Xia Q, Cobblah CNA, Gao J, Xia H. Training Machine Learning Models Through Preserved Decentralization; 2020. p. 465–472.

34. Boneh D, Boyen X, Goh EJ. Hierarchical identity based encryption with constant size ciphertext. In: Annual international conference on the theory and applications of cryptographic techniques. Springer; 2005. p. 440–456.

35. Pointcheval D., Stern J. Security Arguments for Digital Signatures and Blind Signatures. J. Cryptology 13, 361–396 (2000). https://doi.org/10.1007/s001450010003

36. Fan CI, Tseng YF. Anonymous multi-receiver identity-based authenticated encryption with CCA security. Symmetry. 2015; 7(4):1856–1881. https://doi.org/10.3390/sym7041856

37. Pang L, Kou M, Wei M, Li H. Anonymous certificateless multi-receiver signcryption scheme without secure channel. IEEE Access. 2019; 7:84091–84106. https://doi.org/10.1109/ACCESS.2019.2900072

38. Niu S, Niu L, Yang X, Wang C, Jia X. Heterogeneous hybrid signcryption for multi-message and multi-receiver. PloS one. 2017; 12(9):e0184407. https://doi.org/10.1371/journal.pone.0184407 PMID: 28886125

39. Kim I, Hwang SO. Efficient identity-based broadcast signcryption schemes. Security and Communication Networks. 2014; 7(5):914–925. https://doi.org/10.1002/sec.802

40. Obiri IA, Xia Q, Xia H, Affum E, Abla S, Gao J. Personal health records sharing scheme based on attribute based signcryption with data integrity verifiable. Journal of Computer Security. 2021;(Preprint):1–34.