Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18181-4

Enabling secure health information sharing among healthcare organizations by public blockchain

Gianluca Lax[1] · Roberto Nardone[2] · Antonia Russo[1]

Received: 26 April 2023 / Revised: 19 October 2023 / Accepted: 5 January 2024

Abstract
The facilitation of sharing and exchanging patients' health records is a paramount opportunity in e-health, enabling healthcare providers to garner a comprehensive and clear perspective of patients' medical histories without necessitating direct inquiries. Besides this great advantage, it introduces substantial issues on security and privacy, mainly related to unauthorized access to e-health records when different healthcare service providers maintain records. In this paper, we deal with this problem and propose using the blockchain technology (1) to obfuscate the linkage between patients' identities and their e-health records and (2) to grant access to e-health records exclusively to entities authorized by patients themselves. Key outcomes include using a digital identity based on the Electronic Identification, Authentication, and Trust Services Regulation (eIDAS) to control access to these records, and a concrete implementation by adopting the Ethereum blockchain. Our solution relies on using a public blockchain, which is an improvement for the state of the art, in which only private or consortium blockchains have been proposed. The resulting solution has been analyzed, and the effectiveness and affordability of the proposal have been shown.

Keywords Health information security · Digital identity · eIDAS · Smart contract · Ethereum · Solidity

✉ Gianluca Lax
lax@unirc.it

Roberto Nardone
roberto.nardone@uniparthenope.it

Antonia Russo
antonia.russo@unirc.it

[1] Department of Information Engineering, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria, Via Graziella, Località Feo di Vito, Reggio Calabria 89124, Italy

[2] Department of Engineering, University of Naples Parthenope, Isola C4, Centro Direzionale, Napoli 80143, Italy

Published online: 17 January 2024

1 Introduction

The word *e-health* refers to providing health services using digital technology. In e-health, each patient is associated with electronic health records (EHRs) that can be used for diagnosis and monitoring. Doctors may access a patient's e-health records (typically named *personal health records*) generated during the previous visits to have a clear and complete vision of the medical history without needing to ask the patient. In some cases, accessing patients' medical history is possible only if the same healthcare organization has generated e-health records or if a suitable sharing service between two organizations is available. On the other hand, patients go to different healthcare service providers during their lives, resulting in widespread e-health records among many independent repositories, each one maintained by a different healthcare organization. Consequently, a technology able to improve e-health record sharing and exchange among healthcare organizations [1–3] represents a need for the healthcare domain but also a challenge in the research community because several security and privacy problems arise in this new setting. Health data are sensitive [4, 5], and their access should be granted only to authorized entities [6, 7]. Although the protection of EHRs is a primary goal in the healthcare industry, the number of security breaches increases every year [8, 9]. The issue of laws and regulations to protect health information is not sufficient. For example, in 1996, the Health Insurance Portability and Accountability Act was issued in the United States. This act highlighted that the confidential section of electronic medical records needs to be protected and established standards to protect patient's privacy during electronic medical record exchange and sharing [10, 11]. Despite this act, security issues continue to occur in many health organizations [12], and insider abuse is the prevalent cause of privacy breaches [13].

In this scenario, e-health clouds are gaining increasing popularity to facilitate data storage and sharing in healthcare [14, 15]. For example, the proposal described in [16] introduces a three-factor authentication combining password, smart card, and biometrics. This proposal resists various existing attacks, such as impersonation attacks in the registration phase and offline password guessing attacks in the login and password change phase; furthermore, this proposal offers revocation. However, adopting cloud-based solutions leads to a series of challenges, primarily ensuring the security and privacy of highly sensitive health data for the cloud. Even if the cloud is expected to be a trusted party to manage data, it could misbehave because it is under attack or inadequately protected.

Recently, solutions based on *Blockchain* as a distributed public repository storing users' transactions have been proposed [17–19]. Generally, a transaction is a transfer of value among blockchain users who create a wallet with two keys: the private key guarantees the security and authenticity of transactions, whereas the public key generates the wallet identifier (address). Blockchain nodes accept, verify, and validate transactions received from other nodes by running distributed consensus algorithms [20]. Blockchain presents many advantages that could be exploited in public health and social services [21]. The paradigm of Blockchain 2.0 [22] enables the creation and development of smart contracts and pieces of code executed within the entire network. Smart contracts allow users to exchange value and data, automatically verifying conditions and making decisions without third parties. In the context of blockchain-based solutions for healthcare, important research challenges concern how to guarantee that:

1. patient's identity is known without error;
2. this identity is not linkable to an e-health record;
3. only authorized entities can access e-health records.

In this paper, we address these concerns. Concerning the identification of patients, we rely on the concept of identity introduced by the Electronic Identification, Authentication, and Trust Services Regulation (EU) N. 910/2014 (eIDAS) [23], which applies to businesses, citizens, and public authorities all over the EU countries. There are several advantages of using eIDAS-compliant digital identity schemes: one of them is having certain legal validity all around the EU countries.

The second concern is the link between the patient and the record that could be discovered by analyzing information stored in the blockchain. To hide this link, we designed a suitable cryptographic scheme that is proven to be secure.

Concerning the last concern, we observe that most of the solutions proposed in the literature are based on private blockchains, in which only authorized entities can read or write transactions [24]. Other solutions rely on consortium blockchains, which are managed by a limited number of entities and do not implement the distributed nature of the ideal blockchain [25]. In contrast, we rely on a public blockchain and designed a scheme to allow only entities authorized by patients to access their e-health records.

The impact of our solution in terms of economic, social, or human development is relevant: The choice of using a public blockchain allows any party anywhere in the world to access health records securely. Moreover, using a widespread digital identity and a public blockchain combined with a new mechanism for controlled access to e-health records allows us to design a solution many patients can exploit to share their e-health records securely. As a final observation, this research is related to the industrial project iCARE, which aims to build an infrastructure for exchanging health records among different organizations.

The structure of this paper is as follows. Section 2 discusses related work. Section 3 describes the eIDAS ecosystem used in our solution. The proposal's core is presented in Section 4, while Section 5 discusses the validation of the proposed solution. Finally, Section 6 draws conclusions.

2 Related work

This section surveys the literature on privacy and blockchain-based approaches in e-health systems. Blockchain technology can support e-health in overcoming interoperability and security challenges of electronic health records storage and can be a means of designing patient-centric distributed architectures.

As suggested in [26], health information exchange in a trusted environment can solve many challenges in healthcare, such as health-service provider interoperability. In addition, exchanging personal electronic health records immediately affects identifying affected individuals during pandemics. As a matter of fact, healthcare services aim to become patient-centric by facing the security and reliability of patient data controlled by patients and enabling the secure exchange of medical records.

The Health Insurance Portability and Accountability Act [27] establishes privacy and security Rules for properly disclosing protected health information. The privacy rules clearly state the awareness of patients' rights; in particular, information disclosures require patients' authorization.

A framework for authentication and authorization in e-health services is proposed in [28]. It aims to build a secure e-health service system that protects patients' medical records in terms of privacy.

Blockchain-based healthcare systems could support drug supply management, access control for medical activities, and medical record exchange. The authors of [29] and [30] review blockchain-based solutions that exploit some properties of this technology, such as decentralization and absence of a centralized authority, pseudo-anonymity, and heterogeneous transparency.

The authors of [31] exploit the Hyperledger Fabric framework to develop a system that handles patient data. Two blockchains have been proposed: a private one in charge of preserving information about the real identity of the patients and a public one, storing information about patients' health data. The authors have tested the interoperability of the two systems.

An electronic health wallet system based on blockchain and IPFS is presented in [32]. The proposed framework envisions compliance with the GDPR by enhancing the patient-centred paradigm where the patient's privacy results in a critical value. Furthermore, as highlighted in [33], especially in an e-health scenario, data subjects, i.e., patients, must know where and how their data has been stored. A blockchain-based architecture implements this awareness that the authors of [33] propose for e-health applications: the solution provides an efficient privacy-preserving access control mechanism. Again, the technologies mentioned above are also the basis of the solution proposed in [34]. Indeed, dedicated smart contracts enable secure EHRs sharing among different patients and medical providers on a mobile cloud platform.

In order to ensure the security and confidentiality of the patients' EHRs, the authors of [35] use pairing-based cryptography to securely generate tamper-proof of the records shared by a blockchain transaction. This way, authors avoid illegal modification of such items.

E-health data interoperability concerns the issues related to the existing differences in data structures in conventional relational databases. This problem has been investigated in [36] by proposing a unique system for migrating e-health systems to a single blockchain-based ecosystem.

An access control policy algorithm for improving the interoperability of healthcare providers is proposed in [37]. This solution relies on a Hyperledger-based electronic healthcare record-sharing system and focuses on the patient-centric paradigm. Four types of participants (admin, patients, clinicians, and laboratory staff) are identified. Each patient is given the right to read, write, and revoke personal records.

Utilizing the smart contract features, the authors of [38] developed a blockchain model to protect data security and patients' privacy, ensure data provenance, and provide patients full control of their health records. Furthermore, by personalizing data segmentation and creating a list of entities allowed to access their data, their design achieves patient-centric health information exchange.

A blockchain-based data-sharing consent model for access control over e-health data is proposed in [39]. This model provides individuals with consent over their data use and modification through a smart contract and two ontologies that model the consent of users and describe data requests. Accountability of overall participants is guaranteed, and data stored inside the blockchain do not reveal patient identity. Instead, transactions contain details about accesses and purposes (e.g., research, clinical, medical, or biomedical).

To achieve dynamic communication between medical consortium chains, the authors of [40] propose (i) a cross-chain communication mechanism that simplifies the heterogeneous node communication topology and (ii) the construction rules of the node identity credibility path-proof to carry out dynamic construction and verification of the path-proof for cross-chain transactions.

In the study [41], a private blockchain, cloud storage, and several cryptographic mechanisms are exploited to preserve privacy for personal health records. The blockchain stores only record metadata, whereas real encrypted records are stored on the cloud. To access the system, a patient registers to a gateway server responsible for the authentication process. The gateway server is semi-trusted and performs a significant number of operations. In the proposed solution, blockchain only stores the system's metadata and access logs.

The study presented in [25] proposes a blockchain-based privacy-preserving personal health information-sharing scheme. It relies on two blockchains: the former is private, and the latter is a consortium blockchain. The private blockchain stores personal information, whereas the consortium blockchain maintains references to these records. Data, including the records, keywords, and the patients' identities, are public-key encrypted with keyword search.

A decentralized electronic medical records management system leveraging Ethereum is proposed in [42]. This system manages authentication and confidentiality of patient data sharing and allows patients to manage their sensitive data via smart contracts. The framework defines different smart contracts belonging to providers, patients, and other users.

Ancile [43] is a privacy-preserving framework relying on Ethereum and permissioned blockchains managed and controlled by a smaller set of users. The proposed solution is developed to allow patients, providers, and third parties to access medical records in a distributed system. Patients are identified by numerical IDs that are not stored on the blockchain for privacy reasons. Various smart contracts with different roles have been deployed to reduce patient privacy threats. However, the solution suffers from known risks related to adopting a permissioned blockchain.

The authors of [44] propose a model-driven application-level encryption solution to protect the privacy and confidentiality of health data. In this approach, domain experts specify sensitive data that must be protected by encryption, whereas security experts specify the cryptographic parameters used for the encryption in a security configuration. Both specifications support different granularity of data encrypted and appropriate security levels.

This literature review shows how blockchain technology can support access control in managing e-health records over diversified healthcare systems. Our proposal is related to [25, 31, 34, 38] as we face the same problem, which is e-health record privacy. However, the solutions proposed in [25, 31] are mainly built on a private or consortium blockchain, whereas our solution relies on only a public blockchain. Moreover, even if the solutions proposed in [34, 38] rely on Ethereum, they present some evident differences from our proposal. Indeed, in [38], the proposal exploits a permissioned blockchain run by a system administrator to verify each EHR. Concerning [34], the authors envision a central entity, the EHR manager, responsible for controlling blockchain transactions, thus losing the advantage given by blockchain decentralization. In contrast, our proposal relies only on a public blockchain, which is an excellent advantage because it allows any party worldwide to use this solution. To the best of our knowledge, no solution has been proposed combining a public digital identity and a public blockchain to address the privacy and unlinkability of shared e-health records.

3 The eIDAS framework

The Electronic Identification, Authentication, and Trust Services Regulation (EU) N°910/2014 (eIDAS), with reference to electronic identification and trust services for electronic transactions, provides a normative basis to enable secure electronic interactions between businesses, citizens, and public authorities all over EU countries. This Regulation refers to trust service providers established in the Union and to electronic identification schemes that a Member State has notified. Indeed, Member States have to notify their eID scheme (national electronic identification schemes) to the European Commission, which is published in the Official Journal of the European Union. On the other hand, the eIDAS Regulation allows European citizens to access the online services of other EU countries (university services, banking, public administration services, and other online services).

Security, trust, and interoperability of electronic services are considered the main principles of this Regulation. The interoperability [45] regards the definition of interfaces between eIDAS-Nodes belonging to different eID-schemes. Each State Member notified its eID schemes: Estonia was one of the first to notify the European Commission of the adopted solution, which is Estonian eID [46]. The United Kingdom notified the European Commission of using *GOV.UK Verify* [47], based on a federation of private identity providers. In Portugal, Digital Mobile Key [48] has been notified to the European Commission. It allows citizens to sign documents using a smartphone app using their eID smartcards. Paper-based ID cards are replaced by a smartcard-based eID combining four identification numbers (i.e., fiscal, social, health, and civil ID).

SPID [49] is the public system for managing digital identity in Italy. This system allows access to online services of Public Administration for health systems, education, and public administration services, with a single user-password pair. National Identification and Authentication System [50] guarantees electronic identification and secure authentication of users for e-services in Croatia. It enables the identification and authentication of citizens through three entities: issuers of electronic credentials, providers of e-services, and users of e-services.

In the eIDAS framework, eIDAS-Connector and eIDAS-Service need to exchange messages regarding personal and technical attributes to support cross-border identification and authentication processes: to do this, and they use the Security Assertion Markup Language (SAML 2.0) [51]. SAML is an XML-based open-source framework created to securely exchange authentication and authorization information between the service provider and identity or attribute provider. SAML 2.0 specification defines a series of request/response protocols and assertions that allow an application to request or query an assertion or ask a user for authentication.

4 Proposed solution

In this section, we present the solution we propose to share electronic health records securely. First, we present an overview of the approach to allow the reader to understand the proposed solution's idea. Then, we give all the implementation and technical details.

4.1 Overview

An electronic health record is a collection of records storing patient health information digitally. As these records can be generated by different data sources and accessed by different healthcare clinics, these records should be shared among eligible entities. Our solution uses a public blockchain for indexing e-health records and an eIDAS identity scheme to control access to these records. Fig. 1 summarizes our proposal's idea.

On the left of the figure, the indexing of an e-health record is schematized. After an e-health record of a patient is generated (for example, the result of an electrocardiogram), the patient produces a suitable string, which we call *signature*, such that this signature can be generated only by the patient. This signature is sent to the healthcare clinic, which publishes the association between this signature and the e-health record on the blockchain.

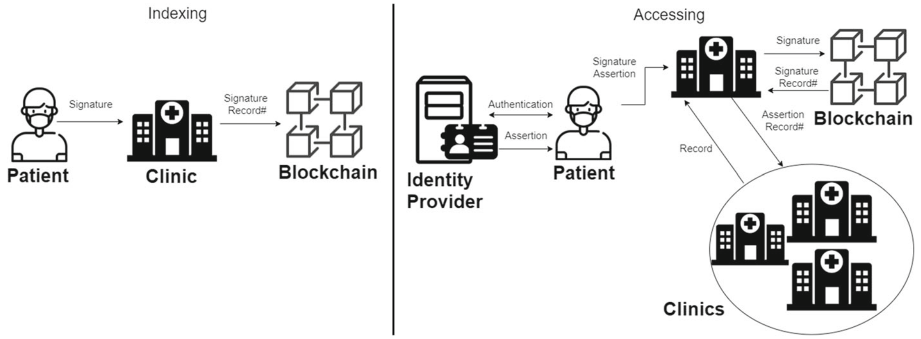

Fig. 1 Overview of the proposed solution

On the right side of Fig. 1, the access to an e-health record is schematized. First, the patient authenticates by an identity provider, which returns a suitable assertion. Then, the doctor who needs to access patients' e-health records receives both such an assertion and the signature generated previously from the patient. The doctor uses the blockchain to obtain the references to the patient's e-health records from the signature. Then, the assertion is used as proof of authorization to access such records. This schematization is simple to understand but does not explain how signatures, authentications, assertions, and references are generated to guarantee the three expected goals. These aspects are discussed in the next section.

4.2 Domain model

To better present and describe the proposed solution, we provide a detailed domain model, described as a UML class diagram, that clarifies the main concepts and relationships among them. The final diagram is depicted in Fig. 2, where the core concepts integral to our solution are represented as UML classes, while their interconnections are depicted as UML associations.

Central to our domain is the `Patient` class, representing individuals in need of or already receiving medical care. Each instance of this class is uniquely identified by an ID, accompanied by personal attributes such as first name, family name, date of birth, and so forth. Every patient is linked to a collection of `Devices` and is correlated with a set of `EHR`s. Notably, each EHR encapsulates a series of `Record`s, with each record emanating from a specific `DataGenerator`. These data generators can span a spectrum of entities, from hospitals to primary care physicians and specialists. Each record, in turn, carries a dedicated reference pointing to its originating data generator. Hence, the class diagram reports a composition between the `EHR` and the `Record` classes, and an association between the `Record` and the `DataGenerator` classes. Each instance of this latter class is identified by an ID, accompanied by the specification type (e.g., hospital, primary care physician, specialist, etc.)

In addition, each patient is connected with the `IdentityProvider` through an additional UML association between classes. This entity stands as a custodian, formulating, sustaining, and orchestrating the user's identity data while also proffering authentication services. The design also considers scenarios where patients may align with multiple Identity Providers, ushering in redundancy which becomes pivotal if an Identity Provider experiences downtime or unavailabilities. Consequently, patients retain the flexibility to select their pre-

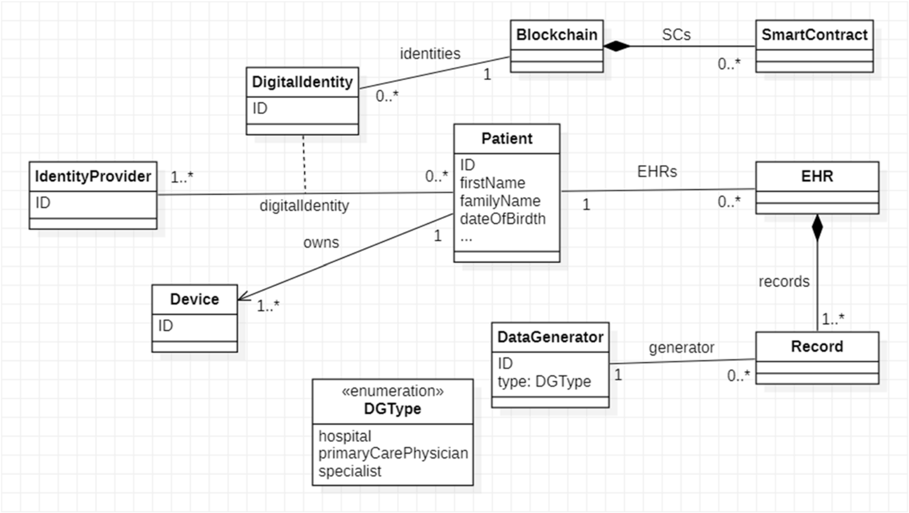

Fig. 2 Domain model

ferred digital identity. Each Identity Provider endows the patient with a distinctive digital identity, serving as a unique identifier for that patient, tethered to that specific identity realm.

Concluding the model is the inclusion of a public `Blockchain` as a UML class, which is a Distributed Ledger primed for the deployment of `Smart Contracts`.

This model clarifies and formalizes all the entities and their interrelationships. This step is necessary to better understand our solution.

4.3 Proposal definition

Our proposed scheme is based on five phases: system setup, identity registration, EHR indexing, EHR request, and EHR release. In the following sub-sections, we describe each phase detailing the exchanged messages. All these phases and interactions are also schematized by the UML sequence diagram reported in Fig. 3.

The notation used in the rest of the paper is shown in Table 1.

4.3.1 System setup

In this phase, the actors perform the operations to initialize the environment. First, all data generators are associated with an identifier (e.g., an incremental counter). In a more general way, we could think of an aggregation of data generators, for example, at the level of cities. In this case, this identifier, say ID_{dg}, could be of the form $ID_{dg} = \langle ID_s, ID_c, N \rangle$, where ID_s and ID_c are references to the state and city in which the data generator is, and N is an incremental integer. For example, ⟨UK, London, 1⟩ could be the reference to the data generator in London associated with the number 1 (e.g., it could be the largest hospital).

In this phase, an asymmetric cryptographic scheme is chosen (e.g., RSA) that will be used when needed.

A one-way hash function $H(x)$ that receives an input x and returns a bit string y with fixed length is also chosen. The requirement of this function is that, given y, it should be

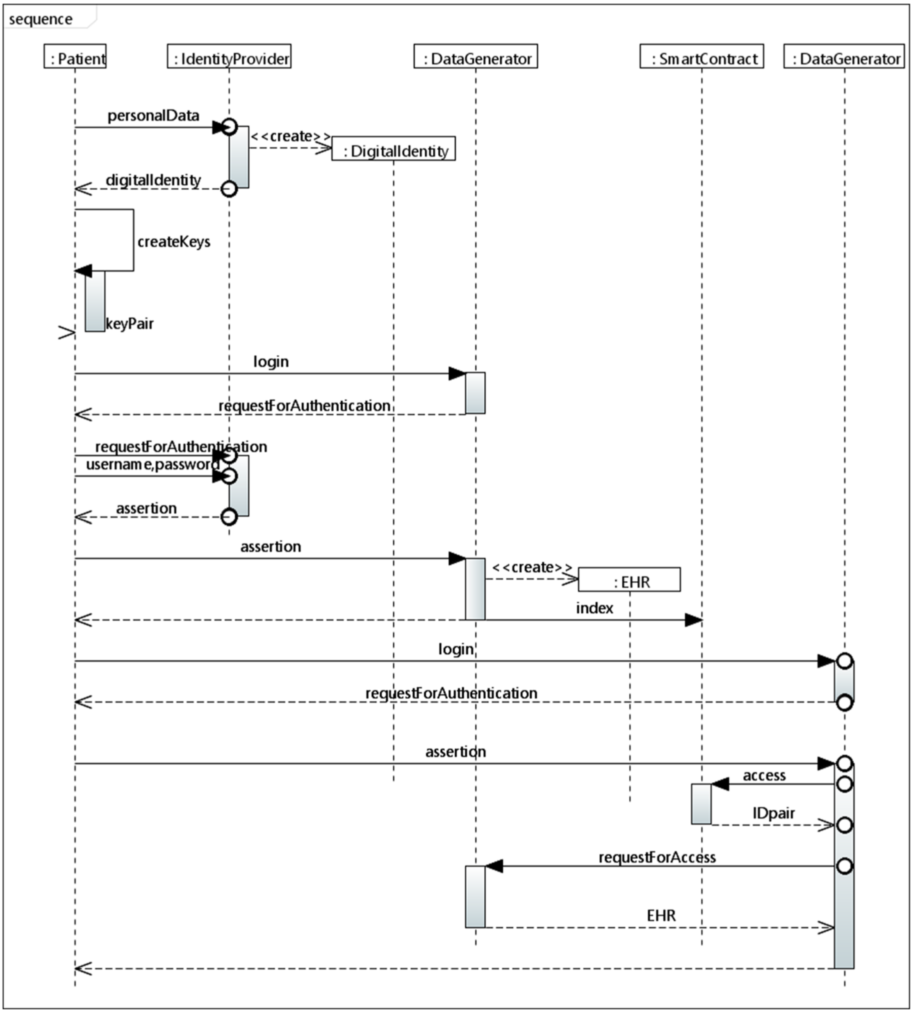

Fig. 3 Sequence diagram describing our solution

difficult to find any message x such that $H(x) = y$ (*one-wayness*). Several hash functions can fulfil this requirement, such as SHA-1, SHA-256, RIPEMD-160.

Finally, a suitable smart contract SC is deployed on the public blockchain, whose functions are described in the following.

4.3.2 Identity registration

A patient performs this phase to obtain a digital identity from an Identity Provider. After verifying the user's data, the Identity Provider issues the digital identity and access information. The digital identity is a set of personal data containing at least the following attributes (according to the eIDAS scheme [52]):

- a string `PersonIdentifier`, which is an identifier of the digital identity;

Table 1 Notations used in the paper

U	User
EHR	Electronic health record
N	Incremental integer
ID_{dg}	Identifier of data generator
ID_s	Identifier of a state
ID_c	Identifier of a city in a state
ID_u	Identifier of U's digital identity
SC	Ethereum smart contract
K_p	Cryptographic public key
K_s	Cryptographic secret key
H	Cryptographic hash function
S	Signature
t	Timestamp
A	Assertion
R	Request for EHR access

- a string `FamilyName`, the surname of the user;
- a string `FirstName`, the name(s) of the user;
- a date `DateOfBirth`, the date and year the user was born.

The user's access information is a pair ⟨username, password⟩, which will be used to authenticate. Moreover, the user generates a pair of asymmetric cryptographic keys (K_p, K_s) of the cryptographic scheme chosen in phase Setup: the private one K_s is known only by the user.

4.3.3 EHR indexing

Consider the case in which a patient U goes to a hospital (i.e., a data generator) for a visit. After the visit, an e-health record of U is generated (for example, the result of an electrocardiogram), and the phase EHR indexing is carried out.

First, U is requested to authenticate by an eIDAS-compliant eID scheme (see Section 3). The user connects to the hospital website and receives a request for authentication, which is forwarded to the Identity Provider. Identity Provider starts a challenge authentication with the user. Suppose the user completed authentication by using the access information (i.e., username and password) received in phase Identity Registration. In that case, the Identity Provider prepares an assertion, which is returned to the user by the Identity Provider and forwarded to the hospital. In case of valid assertion, the user authentication is successful.

Now, U calculates $F = H(S)$, where H is the cryptographic hash function chosen in phase Setup, and S is the signature of the digital identity identifier of U (i.e., the encryption of the string *PersonIdentifier*) computed by the private key of U.

The hospital verifies the validity of the assertion and calls the function `index` of the smart contract SC, which receives $\langle F, ID_{dg}, ID_{ehr}\rangle$, where $F = H(S)$ is defined above, ID_{dg} is the identifier of the data generator as defined in phase Setup and ID_{ehr} is the identifier of the generated e-health record of U. The purpose of the call to this function is to store the mapping between the value F and the pair $\langle ID_{dg}, ID_{ehr}\rangle$ (thus, enabling the possibility to receive this pair starting from F).

Algorithm 1 EHR indexing.

```
Patient sends to Data Generator an authentication request
The authentication request is forwarded to IP
if Patient authenticates then
    IP sends to the patient an assertion
else
    abort
end if
Patient sends to Data Generator the assertion and $F = H(S)$
if assertion is valid then
    Data generator calls index($F, ID_{dg}, ID_{ehr}$)
else
    abort
end if
```

The pseudocode representing this step is shown in Algorithm 1.

4.3.4 EHR Request

Consider now the case in which U goes to another hospital and needs to access the previous e-health records. For this purpose, U is requested to authenticate by an eIDAS-compliant eID scheme. According to the eIDAS Technical Specification [52], the Authentication Request contains the following fields (among others):

1. a unique attribute `IDauthentication_request` generally obtained by a combination of origin and a timestamp;
2. an element `Issuer` that identifies the Service Provider from which the request had origin;
3. an attribute `Destination` that is the address of the contacted Identity Provider for the authentication.

Differently from the standard protocol described above, here the field `IDauthentication_request` is set to the hash value $H(t, ID_{dg}, ID_U)$, where t is the current timestamp, ID_{dg} is the identifier of the data generator, and ID_U is the identifier of the digital identity of U. The purpose of this hash value is to generate an identifier associated with t, ID_{dg}, and ID_U.

After U authenticates, the assertion A is generated by the Identity Provider and returned to the hospital. Moreover, U calculates $F = H(S)$, where H is the cryptographic hash function and S is the signature computed by the private key of U of her/his digital identity identifier (as done in the previous phase).

Now, the hospital calls the function `access` of the smart contract SC, which receives F (i.e., the generated digest) and returns a set of pairs $\langle ID_{dg_i}, ID_{ehr^i_j}\rangle$, in which each element refers to a record of U stored by the data generator ID_{dg_i} (clearly, this function exploits the mapping generated by the function `index`).

After this list is received, a request for accessing the e-health records of the user is sent to each data generator ID_{dg_i}. This request is a tuple $R_i = \langle A, t, ID_{dg}, ID_U, ID_{ehr^i_1}, \ldots, ID_{ehr^i_p}\rangle$, where, we recall, A is the assertion previously generated, t is the timestamp, ID_{dg} is the identifier of the data generator, ID_U is the identifier of the digital identity of U used to generate A, and $ID_{ehr^i_1}, \ldots, ID_{ehr^i_p}$ are the p records of U stored by the data generator ID_{dg_i} (the smart contract call returned these references). It is worth noting that the request

Algorithm 2 EHR request.

```
Patient sends to Data Generator an authentication request having IDauthentication_request = $H(t, ID_{dg}, ID_U)$
The authentication request is forwarded to the IP
if Patient authenticates then
    IP sends to the patient an assertion
else
    abort
end if
Patient sends to Data Generator the assertion $A$ and $F = H(S)$
if assertion is valid then
    Data generator calls access($F$)
else
    abort
end if
Data generator receives a list $L = \langle ID_{dg_i}, ID_{ehr^i_j} \rangle$
for each $ID_{dg_i}, ID_{ehr^i_j} \in L$ do
    Data generator sends to $ID_{dg_i}$ the request $R_i$
end for
```

contains A, which is a proof of the permission given by the patient to access her/his health data (as explained in the next phase).

The pseudocode representing this step is shown in Algorithm 2.

4.3.5 EHR release

When a data generator ID_{dg_i} receives the EHR request $R = \langle A, t, ID_{dg}, ID_U, ID_{ehr^i_1}, \ldots, ID_{ehr^i_p} \rangle$ (defined in the previous step), the following checks are performed to verify the validity of the request:

1. it is verified that A is signed and the signature is not expired as requested by the eIDAS specifications;
2. t, ID_{dg}, ID_U is extracted from R and it is verified that $H(t, ID_{dg}, ID_U)$ is equal to the value of the field `IDauthentication_request`;
3. it is verified that the field `PersonIdentifier` of the assertion is equal to ID_U (i.e., the identifier of U's digital identity).

This concludes the access to the e-health records of the patient, which is granted to a healthcare service provider authorized by the patient.

5 Experiments and validation

To implement our solution, we have to set the system parameters introduced in Section 4.3.1, which are the specific blockchain, the cryptographic hash function H, and the encryption function.

As for the blockchain, we chose *Ethereum* because it is the most used blockchain supporting smart contracts and guaranteeing excellent security standards [53]. Several cryptographic hash functions can fulfil the one-wayness requirement introduced in Section 4.3.1, such as SHA-1, SHA-256, RIPEMD-160. In our case, we chose *Keccak256* because it is supported by Ethereum, where it is used for various purposes, including generating unique identifiers for transactions, blocks, and addresses. Finally, we chose *ECDSA* (Elliptic Curve Digital Signature Algorithm) as an asymmetric cryptographic scheme because it is used to generate public/private key pairs by many blockchains, including Ethereum and Bitcoin.

Once such system parameters are set, we describe the smart contract, which is the core element of the system. We used Solidity [54], an object-oriented and high-level language created for developing smart contracts in Ethereum. We exploited the Remix IDE [55] tool to write, debug, and compile the smart contract. Transactions have been executed and signed by Metamask [56], a web browser plug-in wallet connected to the Ethereum Blockchain. For the sake of presentation, we show in Fig. 4 a basic code of the smart contract implementing our solution.

The struct `record` models an e-health record (Lines 4-7), and the property `records` stores the mapping between patient and e-health records (Line 8). From this code, the reader can understand the implementation of the functions `index` and `access`, which execute the functionalities described in Section 4.

Now we consider the cost of the solution. We measured the cost of deploying the smart contract, which is 547 Micro(ETH) (in October 2023, this is approximately 0.85$), and the cost of the call to the function index is 184 Micro(ETH), which is approximately 28 cents. This result allows us to conclude that the implementation of this smart contract is very cheap.

The evaluation of our proposal is also conducted against the set of requirements we want to guarantee. The first requirement of our proposal is to guarantee that the patient's identity is known without error. This is reached by using an eIDAS-compliant eID scheme, which is universally considered secure provided that the minimum security requirements are respected (e.g., the user does not disclose her/his secret access information).

The second requirement is ensuring that the patient's identity is not linkable to any e-health record. We observe that the only link stored on the blockchain is the tuple $\langle F, ID_{dg}, ID_{ehr} \rangle$ generated in phase EHR Indexing, where $F = H(S)$ is a (ciphered) reference to the patient (i.e., F is the digest of a signature done by the patient) and ID_{dg} and ID_{ehr} refer to the e-health record, respectively. Thanks to the one-wayness of the hash function it is hard to find S starting from F. Moreover, since S can be generated only by the patient (because her/his private key is needed for the generation), F can be also generated only by the patient. In summary, the link between user identity and e-health records exists, but the reference to the user is ciphered and can be decrypted only with the support of the patient.

The last requirement is to guarantee that only authorized entities can access e-health records. Observe that the Identity Provider issues the assertion after identifying the patient

```
 1  pragma solidity ^0.7.4;
 2  pragma experimental ABIEncoderV2;
 3
 4  contract ehealth {
 5      struct record {
 6          uint id_dg;
 7          uint id_ehr;
 8      }
 9      mapping(uint => record []) records;
10
11      function index(uint id, uint id_dg, uint id_ehr) public {
12          record memory _record = record(id_dg,id_ehr);
13          records[id].push(_record);
14      }
15
16      function access(uint _id) public view returns (record [] memory){
17          return records[_id];
18      }
19  }
```

Fig. 4 Sketch of the smart contract

and requiring her/his authorization. Moreover, the field IDauthentication_request is set to $H(t, ID_{dg}, ID_U)$, where t is the timestamp and ID_U is the identifier of the digital identity of U. Before releasing the record, the data generator verifies that 1) the request is not expired and 2) field PersonIdentifier of the assertion is equal to ID_U to ensure that the requested record is relative to the patient to whom the assertion is issued.

6 Discussion and conclusion

In this paper, we proposed a novel solution for allowing the sharing of health records to guarantee that access is granted only to authorized entities and to avoid the linkage between a patient's identity and e-health records. The proposal relies on a public blockchain that represents an entity that can offer a proper trust level of the entire system to patients and offers the needed automatism to the different phases.

The solutions proposed in this context are mainly built on a private or consortium blockchain, which are permissioned blockchain where participating entities have to be known and registered. The need of being registered to the blockchain regards mainly patients, and this requirement limits the spread of the solution. In contrast, our proposal relies only on a public blockchain, which is an excellent advantage because it allows any party worldwide to use this solution.

An advantage of our proposal is related to its simplicity that enables a cheap and open-source implementation in existing blockchain technologies: we measured that the cost of the main operations is very limited (less than 1$).

Another advantage is related to the use of eIDAS-compliant digital identity, which enables the authentication of users by a scheme that is accepted in all EU countries. Moreover, since all actions done on an EHR (specifically, generation of and access to an EHR) are stored in a private way on the blockchain, it is possible to retrieve who generated an EHR and who accessed an EHR with which authorization (thanks to the use of assertions).

On the other hand, to reach such advantages, some negative aspects have been introduced. For example, our scheme expects that patients authenticate before each operation done on their EHR and this has an impact on the invasiveness of the procedure.

Again, the use of a public blockchain instead of a private or consortium blockchain introduces both a (yet small) cost for each transaction and a delay in the time occurring to complete registration or access to an EHR. This delay in the case of Ethereum is 10 seconds on average. We believe that this small delay is tolerable in the considered scenario. Indeed, the time taken by a doctor to analyze an EHR (for example, magnetic resonance imaging) is typically much more than 10 seconds. Moreover, consider that after the user authenticates, it is not necessary for her/his presence to complete the registration or access to an EHR, which can be done in the background.

Another disadvantage of our scheme concerns the impossibility of removing data once they are published on the blockchain. For example, in case an operator publishes the personal data of a patient instead of the hash, then such data will remain publicly available forever (i.e. until the blockchain runs). However, this is a common problem of any application using blockchain and can be contrasted by suitably implementing and testing software and by improving users' awareness.

Future work includes the implementation of a software module which supports the end-users' actions: this full implementation will allow us to distribute and validate the whole system. This activity could also highlight the need for additional functionalities that could increase the attractiveness of the proposed solution.

Author Contributions All authors conceived and designed the proposal. G.L. and R.N. contributed to the methodology. G.L. and A.R. performed the analysis. G.L., R.N. and A.R. wrote the manuscript text. R.N. and A.R. prepared figures and supplementary materials. All authors reviewed the manuscript.

Funding Open access funding provided by Università degli Studi Mediterranea di Reggio Calabria within the CRUI-CARE Agreement. This work was partially supported by "iCARE" project (CUP J39J14001400007) - action 10.5.12 - funded within POR FESR FSE 2014/2020 of Calabria Region with the participation of European Community Resources of FESR and FSE, of Italy and of Calabria.

Data Availability Data transparency is not applicable.

Code Availability Software application or custom code is not applicable.

Declarations

Competing of interest The authors have no financial or proprietary interests in any material discussed in this article.

References

1. Vaishnav R, Panditi MDD, Dhiman V, Aarthy CCJ, Kumari YS, Mohiddin MK (2022) Data security in healthcare management analysis and future prospects. Mater Today Proc 51:2202–2206
2. Rostami M, Oussalah M, Berahmand K, Farrahi V (2023) Community detection algorithms in healthcare applications: A systematic review. IEEE Access
3. Venkatesh R, Savadatti Hanumantha B (2023) Electronic medical records protection framework based on quantum blockchain for multiple hospitals. Multimedia Tools and Applications, pp 1–14
4. Dickerson JE (2022) Privacy, confidentiality, and security of healthcare information. Anaesthesia & Intensive Care Medicine
5. Sheikhpour R, Berahmand K, Forouzandeh S (2023) Hessian-based semi-supervised feature selection using generalized uncorrelated constraint. Knowl-Based Syst 269:110521
6. Kelbert F, Pretschner A (2018) Data usage control for distributed systems. ACM Trans Priv Secur 21(3):12–11232. https://doi.org/10.1145/3183342
7. Karegar F, Pettersson JS, Fischer-Hübner S (2020) The dilemma of user engagement in privacy notices: Effects of interaction modes and habituation on user attention. ACM Trans Priv Secur 23(1). https://doi.org/10.1145/3372296
8. Nduma BN, Ambe S, Ekhator C, Fonkem E, Basil NN, Ekhator C (2022) Health records database and inherent security concerns: A review of the literature. Cureus Journal of Medical Science 14(10)
9. Abouelmehdi K, Beni-Hessane A, Khaloufi H (2018) Big healthcare data: preserving security and privacy. J Big Data 5(1):1–18
10. Paul M, Maglaras L, Ferrag MA, AlMomani I (2023) Digitization of healthcare sector: A study on privacy and security concerns. ICT Express
11. US Department of Health and Human Services (1996) Health insurance portability and accountability act of 1996. Public law 104:191

12. Blanke SJ, McGrady E (2016) When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. J Healthc Risk Manag 36(1):14–24
13. Kim J, Park EH, Park YS, Chun KH, Wiles LL (2021) Prosocial rule breaking on health information security at healthcare organisations in south korea. Information Systems Journal
14. Abbas A, Khan SU (2014) A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J Biomed Health Inform 18(4):1431–1441
15. Li Z-R, Chang E-C, Huang K-H, Lai F (2011) A secure electronic medical record sharing mechanism in the cloud computing platform. In: Consumer electronics (ISCE), 2011 IEEE 15th international symposium on, pp 98–103. IEEE
16. Jiang Q, Khan MK, Lu X, Ma J, He D (2016) A privacy preserving three-factor authentication protocol for e-health clouds. J Supercomput 72(10):3826–3849
17. Mamun Q (2022) Blockchain technology in the future of healthcare. Smart Health 23:100223
18. Mahajan HB, Rashid AS, Junnarkar AA, Uke N, Deshpande SD, Futane PR, Alkhayyat A, Alhayani B (2022) Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. Applied Nanoscience, pp 1–14
19. Mahajan HB (2022) Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: solutions, challenges, and future roadmap. Wirel Pers Commun 126(3):2425–2446
20. Xiao Y, Zhang N, Lou W, Hou YT (2020) A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor 22(2):1432–1465
21. Al Mamun A, Azam S, Gritti C (2022) Blockchain-based electronic health records management: a comprehensive review and future research direction. IEEE Access 10:5768–5789
22. Ethereum (2021) Welcome to ethereum. https://www.ethereum.org
23. eIDAS Observatory (2014) eIDAS Regulation (Regulation (EU) N°910/2014). https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
24. Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X (2017) Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. Information 8(2):44
25. Zhang A, Lin X (2018) Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Med Syst 42(8):140
26. Vest JR, Gamm LD (2010) Health information exchange: persistent challenges and new strategies. J Am Med Inform Assoc 17(3):288–294
27. Edemekong P, Annamaraju P, Haydel M (2020) Health insurance portability and accountability act. StatPearls
28. Han S, Skinner G, Potdar V, Chang E (2006) A framework of authentication and authorization for e-health services. In: Proceedings of the 3rd ACM workshop on secure web services, pp 105–106. ACM
29. Alonso SG, Arambarri J, López-Coronado M, de laTorre Díez I (2019) Proposing new blockchain challenges in ehealth. J Med Syst 43(3):64
30. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L (2018) A systematic review of the use of blockchain in healthcare. Symmetry 10(10):470
31. Hirtan L, Krawiec P, Dobre C, Batalla JM (2019) Blockchain-based approach for e-health data access management with privacy protection. In: 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp 1–7. IEEE
32. Alamri B, Javed IT, Margaria T (2021) A gdpr-compliant framework for iot-based personal health records using blockchain. In: 2021 11th IFIP international conference on new technologies, mobility and security (NTMS), pp 1–5. IEEE
33. Hossein KM, Esmaeili ME, Dargahi T, et al (2019) Blockchain-based privacy-preserving healthcare architecture. In: 2019 IEEE canadian conference of electrical and computer engineering (CCECE), pp 1–4. IEEE
34. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2019) Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE Access 7:66792–66806
35. Zhang G, Yang Z, Liu W (2022) Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput Netw 203:108586
36. Biswas S, Sharif K, Li F, Latif Z, Kanhere SS, Mohanty SP (2020) Interoperability and synchronization management of blockchain-based decentralized e-health systems. IEEE Trans Eng Manag 67(4):1363–1376
37. Tanwar S, Parekh K, Evans R (2020) Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Int J Inf Secur Appl 50:102407
38. Zhuang Y, Sheets LR, Chen Y-W, Shae Z-Y, Tsai JJ, Shyu C-R (V) A patient-centric health information exchange framework using blockchain technology. IEEE J Biomed Health Inform 24(8):2169–2176

39. Jaiman V, Urovi V (2020) A consent model for blockchain-based health data sharing platforms. IEEE Access 8:143734–143745
40. Qiao R, Luo X-Y, Zhu S-F, Liu A-D, Yan X-Q, Wang Q-X (2020) Dynamic autonomous cross consortium chain mechanism in e-healthcare. IEEE J Biomed Health Inform 24(8):2157–2168. https://doi.org/10.1109/JBHI.2019.2963437
41. Thwin TT, Vasupongayya S, Gope P (2019) Blockchain-based access control model to preserve privacy for personal health record systems. Sec and Commun Netw 2019. https://doi.org/10.1155/2019/8315614
42. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International conference on open and big data (OBD), pp 25–30 . IEEE
43. Dagher GG, Mohler J, Milojkovic M, Marella PB (2018) Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 39:283–297
44. Ding Y, Klein K (2010) Model-driven application-level encryption for the privacy of e-health data. In: Availability, reliability, and security, 2010. ARES'10 international conference on, pp 341–346. IEEE
45. eIDAS eID Technical Subgroup (2019) eIDAS - Interoperability Architecture. https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf
46. CEFDigital (2018) Estonian eID scheme: Digi-ID. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia
47. Government Digital Service (2020) GOV.UK Verify overview. https://en.wikipedia.org/wiki/GOV.UK_Verify
48. ePortugal (2021) Digital mobile Key in Portugal. https://eportugal.gov.pt/en/servicos/ativar-a-chave-movel-digital
49. Agenzia per l'Italia Digitale (2018) SPID Sistema Pubblico di Identità Digitale. https://www.spid.gov.it/
50. Belić D (2015) National identification and authentication system. http://infoz.ffzg.hr/INFuture/2015/images/papers/1-06%20Belic,%20National%20Identification%20and%20Authentication%20System.pdf
51. OASIS (2008) Security assertion markup language (SAML) V2.0 technical overview. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
52. CEFDigital (2019) eIDAS eID Profile. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile
53. Tiwari S, Dhanda N, Dev H (2023) A real time secured medical management system based on blockchain and internet of things. Meas Sensors 25:100630
54. Solidity (2023) Solidity Documentation. https://docs.soliditylang.org/en/v0.8.21. Accessed 13-October-2023
55. Ethereum R (2023) Remix - Solidity IDE. https://remix.ethereum.org. Accessed 13-October-2023
56. Metamask (2023) Metamask Wallet. https://metamask.io. Accessed 13-October-2023

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.