SynCare: An Innovative Remote Patient Monitoring System Secured by Cryptography and Blockchain

Claudio Pighini, Alessio Vezzoni, Simone Mainini, Andrea G. Migliavacca, Alessandro Montanari, Maria R. Guarneri, Enrico G. Caiani, Ambra Cesareo

SynCare: an Innovative Remote Patient Monitoring System secured by Cryptography and Blockchain

Claudio Pighini[1,3] [0000-0003-0677-1781], Alessio Vezzoni [2], Simone Mainini[2], Andrea G. Migliavacca[1], Alessandro Montanari[2], Maria R. Guarneri [1,4], Enrico G. Caiani[3] and Ambra Cesareo[1] [0000-0003-4334-7488]

[1] LifeCharger Srl, Via Pico della Mirandola, 8/B, 20151 Milano, Italy
cpighini@lifecharger.eu, acesareo@lifecharger.eu
[2] LiberActa Srl, Via Aurelio Saffi 21,20123 Milano, Italy
simone.mainini@liberacta.com, alessio.vezzoni@liberacta.com
[3] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milan, Italy
[4] Dipartimento di Design, Politecnico di Milano, 20133 Milan, Italy

Abstract. Remote patient monitoring involves the collection of patient-generated health data, using sensors/devices and mobile apps, to allow observation of patient's health status, also outside healthcare environments. The challenge in this field is to facilitate patient-centric data storing, sharing, and retrieving, with high attention to personal, sensitive data privacy and protection. This study presents SynCare, a patient-centered ecosystem developed by LifeCharger, for secure health-related data recording and remote patient monitoring. SynCare has been developed with the aim of making up a strong loop between patients, healthcare professionals and informal caregivers, building up secure channels for data sharing and supporting the patients in the management of their own health and related data. The system includes: 1) a mobile app for the patient, offering different features supporting the therapy and allowing the management of consents to share key data with the healthcare professionals and/or caregivers, 2) a database on Cloud, storing all the encrypted, sensitive health-data, 3) public Ethereum blockchain to validate the data sharing consents, 4) a clinical dashboard developed as a web application whose main purpose is to allow healthcare professional to display and analyze the data collected by the patient through the mobile app. The SynCare ecosystem implements a software developed by LiberActa srl to asynchronously load the anonymous consent data on the Ethereum public blockchain, decoupling the user experience from the blockchain interaction, which can be slow, without compromising the data security.

Keywords: Cyber security, Smart contract, Blockchain, Tele-monitoring.

1 Introduction

Data is the new gold: it is continuously collected and analyzed, to derive information which companies and organization are willing to buy. Centralized organizations – both public and private, collect huge amount of personal and sensitive information and individuals have little or no control over the data that is stored about them and how it is used. There is, consequently, a growing public concern about user privacy. This also applies to health data and, even more, to patient-generated health data. In recent years there has been the multiplication and spread of health mobile apps and wearable devices capable of measuring vital and physiological parameters, leading to a powerful flood of data, which can be used for medical issues related research and to improve the care paths. Also, the present COVID-19 pandemic accelerated the rise of telemedicine, telehealth and health tele-monitoring services [1-3]. Healthcare professionals (HP) started or increased the use of ICT, such as email, text messages and video technology, to communicate with patients, sending prescriptions, monitoring symptoms, and giving medical consultations. In the name of the need to face the emergency, regulatory standard on ethics, privacy and data protection have been temporarily relaxed to allow this shift to socially distanced care [4,5]. Nevertheless, attention to personal, sensible data privacy and protection must be re-established and, in this context, methods and application to favor secure exchange of data between parties (e.g., patient, general practitioners, medical specialists, hospitals, therapists, etc.) are urgently needed.

In this field Blockchain technology can play a key role. Since it was originally introduced and applied to the financial field [6], blockchain technology has gained substantial attention and the interest for its application in diverse fields has constantly increased. The working principle of the Blockchain can be explained using its original application field: Bitcoin transactions. Let's think to the Bitcoin Blockchain as an interconnected collection of digital wallets [7]. A hypothetic transaction of Bitcoins from wallet A to wallet B is simultaneously shared with all other wallets ('miners') in the underlying Bitcoin Blockchain, which use a cryptographic algorithm to validate the transaction. Once a transaction is validated by a certain number of miners, it is stored in a block, which contains the details of the transactions (e.g., transferred sum, ownership, etc.), and marked with a time stamp and a cryptographic hash (a mathematically generated alphanumeric string) of the data. This block is added to the end of the blockchain, which is followed by the transfer of assets (e.g., bitcoins) to the receiving party. The cryptographic hash plays a crucial role in the blockchain mechanism because it permits to create a distinct, digital signature that is unique to the current block of data and, at the same time is created starting from the hash of the previous block, defining a secure link between consecutive blocks (a chain). Thanks to this mechanism malicious changes are prevented from being made to the blockchain ledger and the information related to all previous transactions are completely transparent [7,8]. Now, let's change the digital asset of the example and consider performing transaction of data. Blockchain offers various application possibilities, ranging from management of Electronic Medical Records (EMRs) to Remote Patient Monitoring (RPM) solutions.

This study presents SynCare, a user-centric, secure system for health-related data recording and remote patient monitoring, focusing on the methods and solutions we developed and applied to allows safe exchange of data between patients and healthcare professionals, and to manage data sharing consents by using smart contracts registered on blockchain. The paper is outlined as follows: “Related work” will discuss the existing literature related to this topic, considering the most common applications of blockchain in healthcare. Section “System design” describes the architecture of the whole healthcare ecosystem SynCare, while “Implementation” specifically focuses on methodological aspects of cybersecurity and privacy solutions implemented in SynCare. Section “Discussion” will contain a comprehensive analysis of our system, including a comparison to other previous solutions, advantages, and limitations. Section “Conclusion and future work” concludes the paper and discusses future work.

2 Related Work

Among the biomedical/health care applications of blockchain technology, one of the most popular is management of EMRs [9].

Healthcare in fact suffers from a data silo problem. Patients leave data scattered across various jurisdictions, moving from one provider’s data silo to another. This has consequences not only for the patient, that lose easy access to past data and can interact with them in a broken manner, but also for organizations interested in using AI technology applied to large amount of labeled, clinical data from many sources to improve patient care and help clinicians.

The aim of applying blockchain-based technology in this case is to build a decentralized database management system where hospitals, providers, patients, and other relevant parties can store, share, exchange, and analyze data. One implementation example is Guardtime [10], a Netherland-based data security firm, which provided a blockchain-based system which links Electronic Health Record (EHR) data of patients with their blockchain-based identities. This system has been used in Estonia to secure 1 million health records.

Another known implementation is MedRec project [11]. Medication Reconciliation is a structured process in which Healthcare Providers partner with patients and their family/caregivers to obtain a complete and accurate, up-to-date list of the patient’s medications which is then reconciled with admission, transfer and discharge orders. Blockchain implementation in MedRec project tried to facilitate this process moving from a slow access to fragmented medical data managed by healthcare providers to a system based on a decentralized approach to managing permissions, authorization, and data sharing between healthcare systems, based on patient agency.

Via smart contracts on an Ethereum blockchain, MedRec allows to log patient-provider relationships that associate a medical record with viewing permissions and data retrieval instructions for execution on external databases. Using this mechanism, providers can add a new record associated with a particular patient, and patients can authorize sharing of records between providers. This approach allows patients to know

and decide who can access their healthcare data, acquire copies of their healthcare records or transferring them to another healthcare provider. Although it has been only tested as a proof of concept with medication data, MedRec demonstrated how biomedical and clinical research outcomes may significantly benefit from the application of blockchain to provide rapid, secure access to longitudinal research data. Other examples of application of blockchain in the field of EMR management tried to address the limitations of this approach, namely lack of interoperability among different blockchain-based EMR solutions (lack of standard), scalability (high volume of clinical data), data security and privacy [12-25].

Another use case involves the application of blockchain technology to facilitate remote patient monitoring (RPM) [9]. RPM involves the collection of patient-generated health data, using sensors/devices and mobile apps, to allow remote monitoring of patient's health status, also outside healthcare environments. The aim in this field is to facilitate patient-centric data storing, sharing and retrieving, in agreement with the European General Data Protection Regulation (GDPR) which prohibits the processing of sensitive personal data of patients unless explicit consent is given by the patients. In a recent work Yue et al. [26] proposed an App architecture which allows patient to own, control and share their own data easily and securely by using blockchain technology. Healthbank is a Swiss digital health startup which offers its users a platform on which they can store and manage their health information in a secure environment [27,28]. The data sovereignty lies fully in the hands of the user. As a next step, Healthbank plans to consistently apply and implement Blockchain technology for the underlying business model. Using a private blockchain based on the Ethereum protocol, Griggs et al. created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain [29]. In another work, Liang et al. [30] propose a mobile, patient-centered, blockchain-based system for personal health data sharing. This system is as a permissioned, private blockchain network developed on IBM Blockchain's Hyperledger Fabric. Similar solutions were applied for diabetic patients' monitoring [31] and cognitive behavioural therapy for insomnia [32]. Uddin et al. proposed a system for continuous RPM [33] and data sharing based on blockchain and end-to-end architecture.

3 System Design

SynCare is a patient-centered ecosystem for RPM developed by LifeCharger srl, born to 1) facilitate patient's self-monitoring and remote patient monitoring in chronic diseases, 2) support therapeutic alliance between patients and HPs and, 3) improve patients' engagement and therapeutic adherence for chronic patients or patients performing at-home therapies. To do this it is extremely important to maintain a loop between patients, healthcare professionals and informal caregivers. The main goals for such an ecosystem should be to:

1) build up secure channels for data sharing, in compliance with GDPR
2) support the patients in the management of their own health data

3) clearly define the digital health services, circumscribing the doctor-patient relationship. This is fundamental to guarantee to the healthcare professional the possibility to report the services provided, referring to specific tariffs, also defining the responsibilities connected to these services.

4) as LifeCharger srl, provide the above-mentioned services/ecosystem for the subscribed end-users, acting as a normal third party, without the need to view users' data without a user explicit consent.

Therefore, access to patients' data will be regulated, through the creation of informed digital consents, to clearly circumscribe a digital medical service. These informed digital consents must be traceable, transparent, and not tampered with, but must withdrawable, in compliance with GDPR.

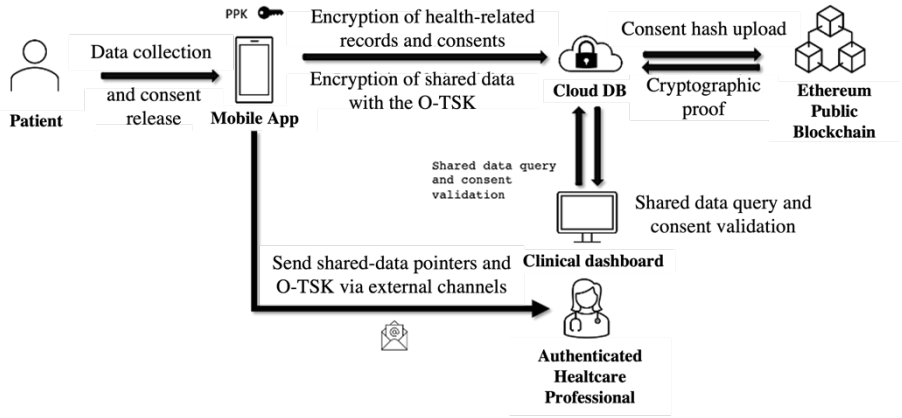

Fig. 1. Architecture and components of the SynCare ecosystem

The main components of the SynCare ecosystem are the following (Fig.1):

- mobile app for the patient
- database on Cloud, storing all the encrypted, sensitive health-data
- public Ethereum blockchain to validate the data sharing consents
- dashboard for the healthcare professionals

The mobile app offers different features to patients; among others: 1) notifications to remind of drugs' intake or activities to perform, 2) a virtual diary to record and report symptoms, measurements of physiologic parameter, performed activities, visits and exams, 3) digital questionnaires, 4) medical reports manager, 5) management of online prescriptions, exams and visits reservation, drug ordering. All the data that are inserted and managed by the app are locally encrypted and then uploaded to a Cloud DB. Data can be subsequently decrypted and visualized only by the patient by using a private key saved on the smartphone. The patient can decide to share such data with third parties, such as a healthcare professional or an informal caregiver, signing a digital data sharing consent through the mobile app. This process can be applied to different use cases, ranging from remote patient monitoring and telemedicine to participation in research experimentations. To ensure that patients can be confident the signed consent is the one they agreed to use and hasn't been tampered with, our solution uses smart contracts as

a ledger of the signed sharing consents. A smart contract is a transaction protocol stored in a blockchain, which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement, without any trusted intermediary's involvement or time loss. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents. Moreover, considered that there's no third party involved, and the encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit. Finally, blockchain transaction records are encrypted, which makes them very hard to hack. Also, given that each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record. The blockchain gives an objective proof of the timestamp at which the consent was released. Indeed, the blockchain reduces the risk that the timestamp associated to the consent could be manipulated during the signature by an eventual intruding attacker that could get hold of the mobile app's code source.

Once the consent is signed by the patient and uploaded on the blockchain, data can be shared, being encrypted and left securely "off-chain", validated and visualized by means of a clinical dashboard built as a web app.

This design ensures patients have the full control over their own health data and can decide who have access and how they are used.

4 Implementation

The present session will focus on the data-sharing methods implemented within SynCare ecosystem, describing how security and privacy issues have been handled using robust data-encryption, and smart contracts on blockchain.

4.1 Overall flow

At the first run, the mobile app generates a Patient Private Key (PPK), saved inside the secure app local storage. The PPK is composed by an RSA-key pair used to sign the consents and to encrypt an AES secret key. When the patient inserts data within the app, these are encrypted using a One-Time Secret Key (O-TSK), which in turn, is encrypted with an AES encryption algorithm by using the local PPK. The encrypted data, together with the encrypted O-TSK, are then uploaded on the Cloud database, creating the secure health record. The data are saved on the Cloud and not on the smartphone for different reasons: 1) ensuring a light app memory, 2) saving space during data sharing (creating the shared data packet and sending procedure), 3) have a data backup in case the phone is lost by the user.

Through this mechanism, the patient is thus the only actor which can decrypt and visualize its own data using the PPK locally stored on his/her personal device. Whenever the patient signs a specific digital consent to share the data with a third party, the mobile app will automatically create the cryptographic hash of the signed consent,

feeding the hash-generating function with the consent meta-data, and then upload it to the cloud DB. Subsequently, an asynchronous cloud server service will feed a Merkle Tree algorithm with the calculated consent hashes to generate the root hash and the cryptographic proof. This algorithm ascends the tree generating a path hash from each couple of leaves until the root is reached, creating the root hash. The hashes of each path are saved inside the cloud DB, associated with their consent hash, while the root hash is stored inside a smart contract deployed on the public Ethereum blockchain.
Once the consent is signed the data sharing can be triggered; specific functions of the mobile App will 1) query the Cloud DB to find the data specified by the consent, 2) decrypt them on the patient's device, 3) generate a O-TSK, 4) encrypt them again with the O-TSK, and finally 5) upload the new encrypted data (shared data) on the Cloud DB. The O-TSK is concatenated with the pointer to the shared data and sent through external channels (e.g., by email) to the third party. The O-TSK will be used by the third party to decrypt the patient's shared data.

Healthcare professionals are provided with a web app which acts as a clinical dashboard, allowing an intuitive and compact visualization and representation of the shared data, and more importantly, verifying their coherence with what has been specified in the sharing consent signed by the patient.
Every time the patients insert or update their health data inside the mobile app, the latter controls if the data are linked to a signed consent. In the positive case, the app automatically updates the shared data pointed by that consent, allowing the healthcare professional web app to query each time trustable and updated patient health-related data.

4.2 The mobile app

Initial Setup. As anticipated in the previous paragraph, at the first run an initial setup procedure on the mobile app generates the PPK, thus, the RSA private (PvK) / public key (PbK) pair, and an AES 256-bit secret key. The PPK is stored in a secure location, corresponding to the KeyStore on the Android operating system and the KeyChain for the iOS. These are two solutions offered by Google and Apple to memorize private information and lowering the risk of data breach in the case of smartphone hacking.

Once the user has been registered on the mobile app, the SynCare ecosystem associates the user's PBK to his/her public information, such as the email and the user ID. For this reason, every time the user logs in on the app the system checks if the PPK has changed, whether it is due to the change of the device or the deletion of the app. To avoid loss of data in the case of device change or app deletion, and to ensure continuity of use for the users, a backup function has been included, allowing the user to save the PPK encrypted into the cloud DB, and consequently allows its retrieval in case of loss.

The initial setup procedure also includes the signature of an umbrella consent to share data (see "sharing consent" paragraph).

Scheduling. Once the initialization is concluded, the user can start to schedule the activities that are prescribed into the therapy or, if the context provides for it, will receive a machine-readable, structured care plan which specific apps' functions will turn into scheduled activities.

The user can choose among different types of activity and schedule them following the guided procedure offered by the app (Fig. 2).

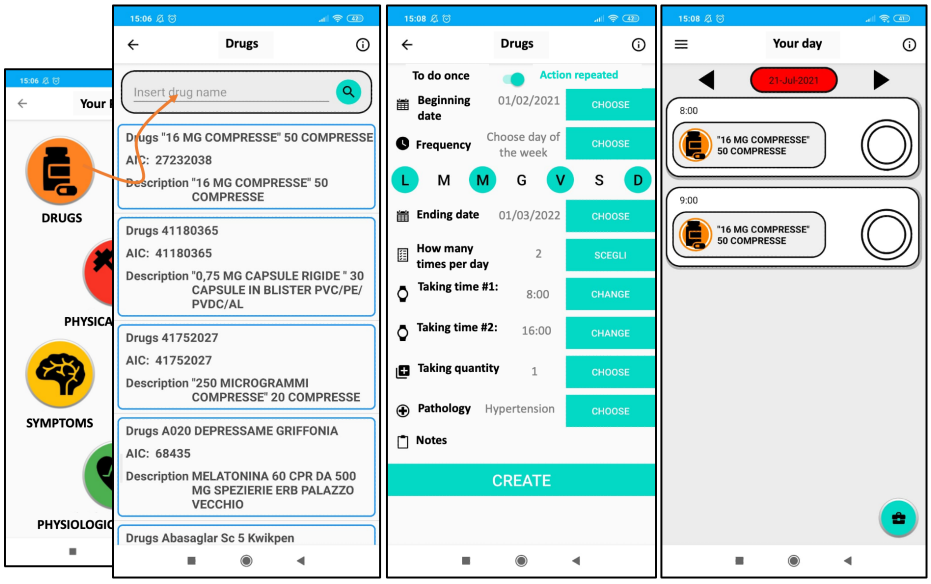

Fig. 2. Scheduling process of the mobile app

Every time an activity is scheduled, the app performs the following steps: 1) encodes the scheduling information following a JSON structure; 2) generates a 256-bit AES key for the symmetric encryption algorithm; 3) encrypts the JSON data structure with the AES key using AES-GCM, 4) encrypts in turn the AES key with the user PbK.

After these operations, a private packet is created with these two components: 1) the AES symmetric key encrypted with the RSA PbK, and 2) the JSON containing the information to be stored, encrypted with the AES symmetric key. This packet is securely saved inside the cloud DB. On the opposite, when the app needs to retrieve the user information to be visualized on the smartphone, the performed steps will be the following: 1) the app asks the LifeCharger cloud DB for the private packet ID; 2) the app uses the RSA PvK to decrypt the part of the packet containing the encrypted AES symmetric key, and 3) the AES symmetric key is used to decrypt the second part of the packet containing the encrypted JSON with the patient's scheduled activity information related to the therapy. This implementation for data encryption/decryption ensures that the patient is the only one who has access and can visualize his/her own data.

Digital Sharing Consents. The SynCare platform has been designed to allow the mobile app to share the patient's health-related data only through the signing of digital sharing consents. Digital sharing consents are smart contracts registered on blockchain which allow to clearly define the contract between the patient, the informal or

professional caregiver or the generic third party with whom the patient wants to share the data. The contract defines:

- Contractors: who owns the data and who can access them
- Type of data shared: it is possible to share one or more datatypes (drugs, symptoms, physiological parameters) or select data with specific tags (e.g., classified per pathology)
- Temporal limits: continuous sharing (real time monitoring), one-shot sharing (visit-related sharing) or periodic sharing (monitoring)
- Finality for which the data are shared and linked data usage (this covers the definition of the legal responsibilities for the healthcare professional in case of medical services

Digital sharing consent can be classified into two main categories:

- **Umbrella sharing consents**: signed just once by the users, typically during the initial setup procedure. This kind of consents are mandatory; this means the user cannot use the app if he/she does not sign this kind of consent. One example of umbrella sharing consent is the one used for research projects, that authorizes LifeCharger srl or other partners of consortium research projects, to analyze the user data for statistical/research purposes or to share collected data with other companies/partners developing modules and components of the overall project platform. In this case the patient/subject who is enrolled in the research must give his/her consent for data sharing and processing, for the purposes and in the manner described in the consent, under penalty of non-participation in the project. Umbrella sharing consents are signed by the users by using the stored PvK.
- **Specific sharing consents**: these consents can be signed by the users, but the non-signature does not preclude the use of the app (see Fig. 3). The user has an active role in this case because he/she decides to share the data collected through the mobile app with a third party, and to do it will sign a specific consent, which describes the kind of data to be shared, the time of sharing (start and end date), the actors involved (sender and recipient) and the finality of use of the data. This kind of consent is typical of the patient-caregiver relationship

Once the patient has agreed to all consent policies, the app creates the signed consent record. Independently from the type of consent, this operation includes: 1) the calculation of a hash starting from the information described into the consent, thus the consent meta-data; 2) the creation of an unique ID that is assigned to the shared packet containing the shared data as UUID; 3) the calculation of the timestamp relative to the moment of consent signing; 4) application of a signature to the consent hash with the RSA PvK, in order to ensure that the data owner has done this operation. These data are added to the signed consent meta-data and saved encrypted into the cloud DB. As the user gave his consent for data sharing, the app will generate the packet that will contain the patient's data to be shared and described by the digital consent. This operation includes: 1) the encoding of the information inside a JSON structure; 2) the creation of a hash of the JSON data; 3) recovery of the PbK and to the package; 4) concatenate the hash with the timestamp; 5) the system signs with the PvK the

concatenated string; 6) the generation of a 256-bit AES key, the O-TSK, which is used to encrypt the JSON part containing the health-related data; 7), finally, the packet of data to be shared is created by combining the encrypted JSON and other transparent anonymous data regarding general info of the consent, thus, the shared packet is saved on SynCare cloud DB.

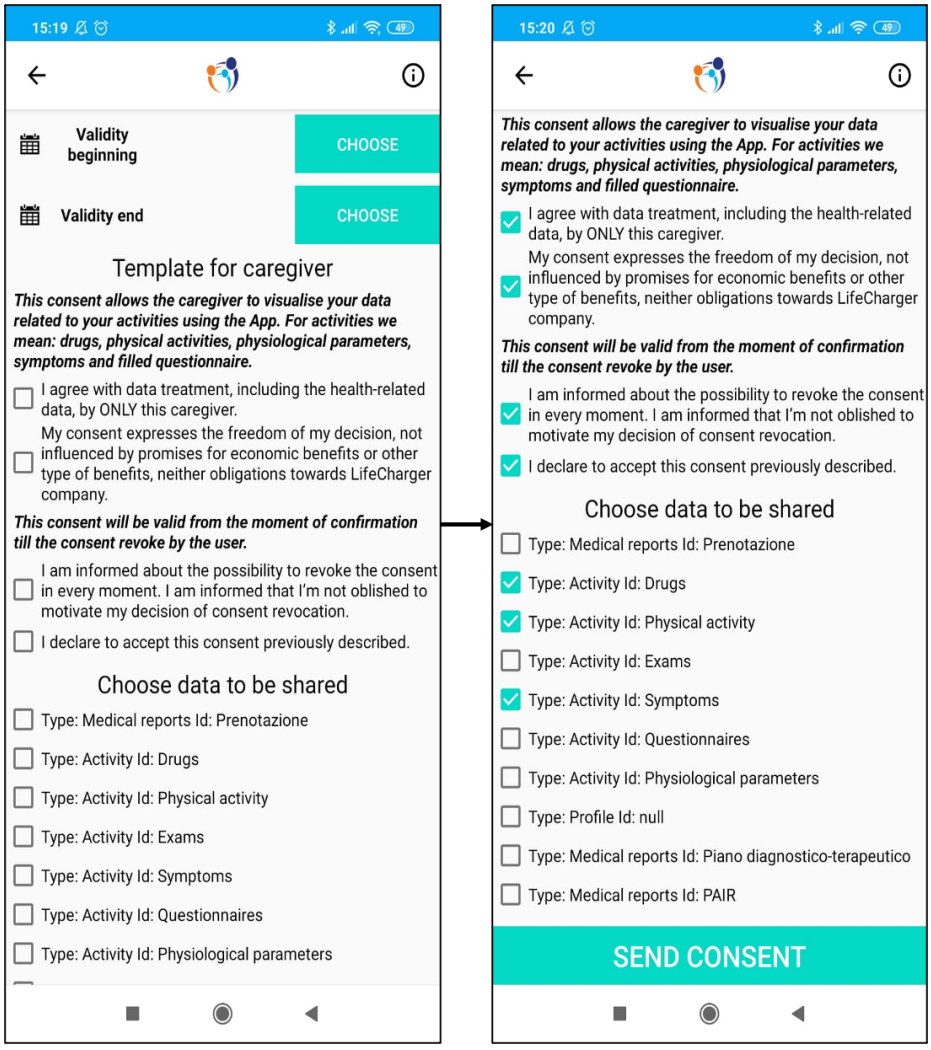

Fig. 3. Consent signing and sending procedure. The figure shows an example of a consent for an informal caregiver

Consent Withdrawal: In compliance with GDPR, our solution foresees the possibility for the patient to withdraw the consent at any time. To allow this, the system keeps track of all the shared data packet linked to each signed sharing consent. When a user

decides to withdraw a previous consent, the linked shared data packets are delated from the DB and the corresponding hash marked as “not valid”, thus the mobile app will stop to share the data packets related to that consent. This means that the linked viewership permissions are modified and the third parties which previously received the link with the O-TSK to decrypt the shared data will not be no longer able to retrieve those data packets.

The data sharing between the app’s user and the third parties inside the SynCare ecosystem starts from the assumption that the shared data can be opened only via browser. Indeed, at the end of the data packet creation that contains the patient’s shared data, the app will generate a link that will be sent via a selected email client into the smartphone. The link il composed of the following parts:

1. the URL of LifeCharger srl https service that provides the clinical dashboard
2. the UUID that identifies the shared packet record, saved into the cloud DB, concatenated to the previous one (according to the syntax implemented by LifeCharger)
3. the "#" and a secret information (O-TSK) needed to recreate the symmetric key to decrypt the message.

This is an example of how the link looks like:

https://share.lifecharger.ey/(UUID)#(SECRET).

By inserting the O-TSK after the “#”, the server will not be able to read the secret key that is used to decrypt the shared data. Thus, LifeCharger acts as clearinghouse during the data sharing process, without the possibility of seeing the shared data among the user and the third parties.

USE CASE: Mario suffers from Parkinson and during his last visit, his neurologist, Dr. Moore suggested that he joins the continuity care program using the SynCare platform. Thus, Mario downloaded the mobile app as suggested by Dr. Moore and registered on it. Subsequently Dr. Moore sent a sharing consent request via web Dashboard. In the request, Dr. Moore asks Mario to digitally sign an in-app consent that defines the relationship of the digital continuity care service: the consent defines that Dr. Moore will send a digital care plan that will be received and visualized by Mario through the mobile app as a structured agenda containing the assigned activities, and they will plan 5 video-visits in the next 12 months. Dr. Moore will monitor the trends and the care path of Mario to define the needed adjustments of the care plan; to do this, he needs to view data collected by Mario regarding the taken drugs, reported symptoms, vital signs, and questionnaires. The consent defines that these data will be accessible for Dr. Moore two days before and two days after the planned video-visits for a total period of 12 months. Mario agrees to all consent policies, signing the consent. From this moment, all data types described by the consent will be encrypted and included in the shared data packet by the mobile app. Two days before the next video visits with Dr. Moore, the app will generate and share with him via email a link containing the pointers to the shared data packet and the key to decrypt the data. He will use this link pointing to the web dashboard, and after authentication with his credentials, he will have access to the data of Mario. Dr. Moore, according to the signed consent, will be able to access and

view the data for two days after the visit, then the sharing data packets will be deleted and will be available again and updated with new data at the next visit. Some weeks after starting using the mobile app, Mario decides to add his son Luca, as an informal caregiver, using the specific functionality of the app. To do this, he must sign another consent, specifying what types of data and how often to share with the child. He decides to share all data in a continuous way with Luca. So, this latter, using the reporting functionality of the app in caregiver mode can view all data regarding the health status and therapeutic path of the father, including pharmacological adherence and vital signs trends.

4.3 The Encrypted Cloud DB

The SynCare cloud DB relies on a non-relational database structure, where data are stored as simple key/value pairs. In particular, the structure of each record inside the SynCare cloud-based DB follows the typical structure of a JSON document.
In general, each record stored by the app is composed of a transparent unencrypted part, that represents the non-sensitive information (the user ID, a hexadecimal string that defines uniquely the patient inside the SynCare ecosystem, different timestamps, and reference keys linking to different collections) and an encrypted part, which encapsulates the obscured sensitive data.
From the previous paragraph, we can identify two types of data saved into the database by the app. The first one is represented by the information that only the user can read through the decryption procedure introduced in paragraph 4.2. The second one is the shared data packet that is stored on the cloud DB at the end of the data sharing procedure, waiting for the retrieval by a third party through the generated link, that is sent via email. In fact, the only way to open and visualize the patient's health-related sensitive data is to receive the mentioned link and, through the adopted web app (see paragraph 4.5), decrypt the patient's data. Consequently, neither the SynCare company owner, LifeCharger srl, nor a general third party, can access the sensitive part saved inside the records without the patient's authorization, given by signing a digital consent.

4.4 The Blockchain consent validation and synchronization

The SynCare ecosystem implements a software developed by LiberActa srl (LA) to upload the anonymous consent data on the Ethereum public blockchain. This software is based upon a cloud backend that can interact through REST APIs and a smart contract deployed on the Ethereum blockchain.
This system aims to memorize on the Ethereum blockchain the past digital consent data signed through the mobile app. For this reason, the software was written to decouple the consent signing phase and the storage on the public blockchain. In particular, the consent data are passed to the LA backend every time a consent is signed by the mobile app. The consent data are initially saved only into the SynCare cloud DB. Consequently, the LA backend concatenates the received data inside a buffer. When the buffer maximum storage capacity or a certain established time are reached, a process is run to collect the unsaved consent data. This latter generates a Merkle Tree.

The root of the generated Merkle Tree is then saved inside each record of the previously processed consents, together with the cryptographic proof that allows the consent validation. Therefore, the root of the Merkle Tree is stored inside the smart contract, allowing a light transaction into the public blockchain.
At regular intervals, SynCare downloads the cryptographic proofs saved into the LA database, associating them to the relative consents. Thus, to verify the existence of a certain consent on the blockchain, SynCare can simply 1) calculate the consent hash, 2) reconstruct the Merkle Tree root with the provided cryptographic proof, and 3) verify the presence of that root using the smart contract. This process is executed automatically by the SynCare clinical dashboard, without the need for an active user interaction.

4.5 The Clinical Dashboard

The clinical dashboard is a web application whose main purpose is to allow healthcare professionals to visualize the data collected by the patient through the mobile app, allowing to display and analyze the shared data. The Dashboard implements two key features that enforce the privacy and make the exchanges between the patient and the healthcare professional a sort of end-to-end encrypted channel. The first feature is the decryption performed on client side through Javascript code locally on the browser of the healthcare professional. The Dashboard retrieves the encrypted information from the Cloud DB. However, considered that the decryption key O-TSK is communicated by the patient by email or other means external to the SynCare platform and that the decryption is done on the browser, no sensitive information is exposed on the SynCare cloud infrastructure.
The other key feature provided by the Dashboard is a check, done on the client side through Javascript code, certifying that the information shared by the patient matches the consent previously signed. The encrypted shared data, in fact, contains a copy of the consent signed by the patient. It is worth noting that the consent is not just a pure text object but also contains a data structure, that is a formal description of the information that is going to be shared with the consent. It is a simple list of codes each one identifying a specific health information based on an agreed taxonomy.
The Dashboard performs the following checks: 1) the data shared by the patient must match with the data structure of the signed consent, 2) the consent must be signed by the same patient that encrypted the shared data, 3) the consent must have been registered in encrypted form by SynCare, and 4) the consent has been registered on the Blockchain. The SynCare Ethereum Smart Contract doesn't expose sensitive data, in fact only the cryptographic proof of existence of the consent is tracked on the Blockchain. The Dashboard can check if this cryptographic proof matches with the specific consent and provides the corresponding Ethereum transaction ID, so the check can be done externally to SynCare. Eventual failures in the checks described above produce an alert on the Dashboard.

A remarkable aspect of the Dashboard is that both the decryption and the compliance check between consent and shared data are done on client side, that is on the healthcare professional browser, so the users do not need to trust or rely on SynCare, and/or on

the cloud application for these critical tasks. With this mechanism, the client can validate the consent data in automatic and transparent way.
As an additional safety measure the Dashboard needs the healthcare professional to be authenticated. This constraint does not invalidate the end-to-end encrypted channel described above but protects against malicious attempts to steal the decryption keys. In fact, intercepting the O-TSK sent to a healthcare professional without his/her credentials would be useless. Moreover, considered that the system works based on sharing packets (shared data packet) each packet linked to a specific consent, is encrypted with a different O-TSK, therefore having the credentials to access the client and a link with the O-TSK, will allow the decryption of only the data packet specified in that specific consent.

5 Discussion

Scalability of blockchain-based healthcare solutions is a major challenge especially in relation to the volume of data involved. It is not optimal, or even practicable in some cases, to store the high-volume biomedical data on blockchain as this is bound to cause serious performance degradation [9]. To solve this problem, our solution uses a smart contract registered on a public blockchain as a ledger of the sharing consents signed by the patient. All the patient's sensitive data are left "off-chain" and opportunely encrypted to be stored and shared. This solution allows fast and lightweight blockchain transactions, reducing the costs of each blockchain consent storage and simplifying the maintenance of the smart contract. Moreover, contrarily to the majority of the existing implementations in the same field that use private [11,26,30-33] or semi-private [29] blockchains, our solution exploits the advantages of the public Ethereum blockchain, namely robustness and stability, without affecting privacy and data security, having the sensitive data saved encrypted off-chain. Moreover, in most of the solutions using private blockchain data are saved not encrypted, this means that whoever has the access credentials can see private information of patients. As a final advantage of using a public Ethereum blockchain we mention the savings in maintenance costs.
For what concerns "off-chain" data security, our solution applies data encryption with AES using 256 bit one-time, disposable, secret key. This means that each time data is encrypted a new key is used; moreover, the private key saved on the user's smartphone is used to encrypt the secret key which has encrypted the data ensuring greater data security.
Considering the data sharing function, our solution puts the patient at the center of the process: in fact, the user decides which data to send by consent creation or acceptance of consent generated by a third party. The system has been designed in such a way that it is always the user that initializes the data sharing, in fact the data package created is linked to the consent for data sharing signed by the patient.
An important limitation of previous implementations is the limited speed of the blockchain-based transactions, which can introduce some significant latency. Our solution tries to reduce this problem allowing to create an asynchronous loading of consent data inside the public blockchain, decoupling the user experience from the

blockchain interaction, which can be slow, without compromising the data security. Moreover, by collecting all the consent data into the LA buffer and memorizing them as a Merkle Tree root, the cost of every transaction inside the blockchain is drastically reduced.
The main limitation of the system regards the time of encryption/decryption of data, which in the current version of the system, is performed each time the user opens the calendar function. This means long charging times when shifting from a function to another of the mobile app. This problem worsens increasing the amount of data inserted by the user.

6 Conclusions and future work

To conclude, SynCare allows continuous and trustable patient remote monitoring, in compliance with privacy normative and leaving to patients the full control of data-access permissions. Data sharing consents managed as smart contracts allow to clearly define which data are shared with the healthcare professionals, the temporal characteristics of the data-sharing (e.g., continuous, one-shot, starting and ending dates), and how the data are used (which performance is expected). This is the first step for a clear definition of the medical performance in telemedicine, including responsibility and accountability, and could foster the spread of telemedicine and teleassistance services. Next steps of development will focus on speeding up and optimizing the processes of encryption/decryption of data to ameliorate the user experience avoiding long charging time when opening the app and switching between app's functionalities. As already mentioned in the discussion, the latency introduced by encryption/decryption process is currently the main limitation of the system that worsen the user experience. To ameliorate this aspect, we introduced a local Realm on the smartphone, where a subset of useful data is saved unencrypted. As a future work, we plan to make specific performance tests to quantify the latency introduced by the blockchain-based transactions, including encryption/decryption phases. On the other hand, we are working on additional features: the first one regards the refinement of the consent management, introducing the fundamental possibility to modify and/or withdraw the consent, with consequent change of viewership permissions. Another improvement wants to take advantage of the use of blockchain to provide to the patient/user a log of all data accesses to the shared data. This would add transparency to patient-provider relationships while keeping participants informed and engaged in the evolution/use of their records. Finally, we plan to further increase the security of our solution, trying to minimize the possibility of external attacks aimed at manipulating the source code of the app. To do this we will perform a security analysis with an attacker model.

References

1. Lin, C.; Bookman, K.; Sieja, A.; Markley, K.; Altman, R.L.; Sippel, J.; Perica, K.; Reece, L.; Davis, C.; Horowitz, E. Clinical Informatics Accelerates Health

System Adaptation to the COVID-19 Pandemic: Examples from Colorado. *Journal of the American Medical Informatics Association, 27*, 1955-1963 (2020).
2. Perrone, G.; Zerbo, S.; Bilotta, C.; Malta, G.; Argo, A. Telemedicine during Covid-19 Pandemic: Advantage Or Critical Issue? *Med. Leg.* 2020*, 88*, 76-77.
3. World Health Organization. *Responding to community spread of COVID-19: interim guidance, 7 March 2020 (*2020).
4. Bassan, S. Data Privacy Considerations for Telehealth Consumers Amid COVID-19. *Journal of Law and the Biosciences, 7*, lsaa075 (2020).
5. Martinez-Martin, N.; Dasgupta, I.; Carter, A.; Chandler, J.A.; Kellmeyer, P.; Kreitmair, K.; Weiss, A.; Cabrera, L.Y. Ethics of Digital Mental Health during COVID-19: Crisis and Opportunities. *JMIR mental health, 7*, e23776 (2020).
6. Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system (*2019).
7. Dwyer, G.P. The Economics of Bitcoin and Similar Private Digital Currencies. *Journal of financial stability, 17*, 81-91 (2015).
8. Böhme, R.; Christin, N.; Edelman, B.; Moore, T. Bitcoin: Economics, Technology, and Governance. *Journal of economic Perspectives, 29*, 213-238 (2015).
9. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. In Healthcare. Multidisciplinary Digital Publishing Institute, Vol. 7. No. 2. (2019).
10. Mettler, M. Blockchain Technology in Healthcare: The Revolution Starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). (2016)
11. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using Blockchain for Medical Data Access and Permission Management. In 2016 2nd International Conference on Open and Big Data (OBD); pp. 25-30 (2016)
12. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing, 5*, 31-37 (2018).
13. Kaur, H.; Alam, M.A.; Jameel, R.; Mourya, A.K.; Chang, V. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *J. Med. Syst., 42*, 1-11 (2018).
14. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information, 8*, 44 (2017).
15. Milojkovic, M. Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records using Blockchain Technology. (2018).
16. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records using Blockchain Technology. *Sustainable cities and society, 39*, 283-297 (2018).
17. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.; de Albuquerque, Victor Hugo C. A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cognitive Systems Research, 52*, 1-11 (2018).

18. Li, H.; Zhu, L.; Shen, M.; Gao, F.; Tao, X.; Liu, S. Blockchain-Based Data Preservation System for Medical Data. *J. Med. Syst., 42*, 1-13 (2018).
19. Allanson, J.; Fairclough, S.H. A Research Agenda for Physiological Computing. *Interact Comput, 16*, 857-878 (2004).
20. Wang, H.; Song, Y. Secure Cloud-Based EHR System using Attribute-Based Cryptosystem and Blockchain. *J. Med. Syst., 42*, 1-9 (2018).
21. Zhao, H.; Bai, P.; Peng, Y.; Xu, R. Efficient Key Management Scheme for Health Blockchain. *CAAI Transactions on Intelligence Technology, 3*, 114-118 (2018).
22. Zhao, H.; Zhang, Y.; Peng, Y.; Xu, R. Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS); pp. 229-234 (2017).
23. Zhang, X.; Poslad, S. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). In 2018 IEEE International Conference on Communications (ICC); pp. 1-6 (2018).
24. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems Via Consortium Blockchain. *J. Med. Syst., 42*, 1-18 (2018).
25. Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S. Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. 534-543). Springer, Cham. (2017)
26. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst., 40*, 1-8 (2016).
27. Healthbank Homepage, https://www.healthbank.coop, last accessed: 2021/07/22.
28. Nicholm, P.B. Blockchain Applications for Healthcare. https://www.cio.com/article/3042603/blockchain-applications-for-healthcare.html, last accessed: 2021/07/22.
29. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst., 42*, 1-7 (2018).
30. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); pp. 1-5 (2017).
31. Saravanan, M.; Shubha, R.; Marks, A.M.; Iyer, V. SMEAD: A Secured Mobile Enabled Assisting Device for Diabetics Monitoring. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); pp. 1-6 (2017).
32. Ichikawa, D.; Kashiyama, M.; Ueno, T. Tamper-Resistant Mobile Health using Blockchain Technology. *JMIR mHealth and uHealth, 5*, e111 (2017).
33. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture. *IEEE Access, 6*, 32700-32726 (2018).