Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems

Conference Paper · December 2017

CITATIONS
13

READS
613

6 authors, including:

Xueping Liang
University of North Carolina at Greensboro
26 PUBLICATIONS **827** CITATIONS
SEE PROFILE

Sachin Shetty
Old Dominion University
237 PUBLICATIONS **2,040** CITATIONS
SEE PROFILE

Juan Zhao
Vanderbilt University
38 PUBLICATIONS **433** CITATIONS
SEE PROFILE

Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems

Xueping Liang[1,2,3], Sachin Shetty[4], Juan Zhao[3], Daniel Bowden[5], Danyi Li[1]†, Jihong Liu[1]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing, 100190, China
[3]College of Engineering, Tennessee State University, Nashville, TN 37209
[4]Virginia Modeling Analysis and Simulation Center, Old Dominion University, Norfolk, VA 23529
[5]Sentara Healthcare, Norfolk, VA 23455

Abstract. With the increasing development and adoption of wearable devices, people care more about their health conditions than ever before. Both patients and doctors as well as insurance agencies benefit from this advanced technology. However, the emerging wearable devices creates a major concern over health data privacy as data collected from those devices can reflect patients' heath conditions and habits, and could increase the data disclosure risks among the healthcare providers and application vendors. In this paper, we propose using the trusted execution platform enabled by Intel SGX to provide accountability for data access and propose a decentralized approach with blockchain technology to address the privacy concern. By developing a web application for personal health data management (PHDM) systems, the individuals are capable of synchronizing sensor data from wearable devices with online account and controlling data access from any third parties. The protected personal health data and data access records are hashed and anchored to a permanent but secure ledger with platform dependency, ensuring data integrity and accountability. Analysis shows that our approach provides user privacy and accountability with acceptable overhead.

Keywords: Privacy Protection, Healthcare Industry, Access Control, Self-Sovereignty, Trusted Computing, Blockchain, Decentralization, Intel SGX, Accountability

1 Introduction

The rising of wearable technology contributes to the digitalization of the world. Wearable technology refers to networked devices embedded with sensors which can be worn comfortably on the body or even inside the body to collect health

†Corresponding author.

data and tracking activities [20] thus serving as a convenient tool to monitor personal health. From doctors' side, those collected data can be valuable clues for determining the appropriate medical treatment. Besides, Insurance 3.0 [3] rises as a result of analysis on big data. With the availability of rich health data in the cloud, health insurance companies can make more strategic policies according to individual characteristics.

However, challenges are arising since more health data can be collected from both wearable devices and EHR systems. First, patients become more concerned about the privacy of the health data. Many exiting state-of-the-art approaches focus on improving data providers' responsibilities to detect the data disclosure activities, however, it is urgent to protect data access and provide immediate notifications of data disclosure risks. Second, over 300 different EHR systems are in use today, but most of them adopt a centralized architecture which suffers from single point of failure. Meanwhile, there are little or even no communication and cooperation among systems [1]. The isolation between data centers results in the lack of a holistic and thorough view of personal health. It is reported that 62% of insured adults rely on their doctors to manage their health records [1], which limits their ability to interact with other healthcare providers than their primary doctor. Moreover, even though many health providers are supposed to follow rules or laws, such as HIPAA (Health Insurance Portability and Accountability Act of 1996), but there are still many entities which are not covered by any laws. Therefore, it is crucial that any entity that has access to the data should be accountable for their operations on the data and any operations on the data need to be audited.

With the above mentioned issues of data ownership, data isolation and lack of accountability, as well as high privacy risks existing in current EHR systems, patients have little control over their personal health data [10], the notion of Self-Sovereignty [7][13] gains great popularity for dealing with healthcare data issues. To better bring this concept into reality, we adopt two novel technologies, Intel SGX and blockchain, to implement a patient-centric personal health data management system with accountability and decentralization. Intel SGX offers an anonymous key system (AKS) [19] that can generate an anonymous certificate which will then be transmitted to a certification platform for validation. Blockchain technology, where data are stored in a public, distributed and immutable ledger, maintained by a decentralized network of computing nodes, provides a decentralized and permanent record keeping capability, which is critical for data provenance [12] and access control [9] in cloud data protection.

In this paper, we propose a complete patient-centric personal health data management system, allowing patients to collect and manage their health data all in a compliant way. In the development of the system, we take the user ownership of data into consideration and the contribution is as follows.

- **Self-Sovereign Data Ownership.** We adopt the idea of user-centric architecture to control data access and issue permissions. It is the data owner that decides who can acess the data and whether to make the data public

or private, as well as how to validate the data. Token-based verification is utilized to grant one time access to data requested by third parties.
- **Permanent Data Record with Integrity.** We collect data records and submit an abstract of each record to the blockchain network. The records are included in a block and the integrity of the record is guaranteed by the consensus mechanism used in the block mining process.
- **Scalable Data Processing.** The volume of health data collected from wearable devices and user input scales greatly so we propose a high-speed algorithm to improve the efficiency of data processing.
- **Decentralized and Distributed Privacy and Access Control.** We propose a decentralized permission management protocol to deal with each personal health data request. The data access records are stored to provide traceable logs, using blockchain to preserve immutability.
- **Trusted Accountability.** The trusted execution environment provisioned by Intel SGX is utilized to generate a fingerprint for each data access. For medical treatment and insurance enforcement, every action is traceable. Once data leakage is detected, the malicious entity can be identified for investigation.

The rest of the paper is organized as follows. Section 2 introduces the overall system design, including the architecture, system entities, key establishment and system procedures. We describe the token-based access control in Section 3 and decentralized integrity protection and accountability in Section 4. Performance evaluation is presented in Section 5. Section 6 concludes the paper.

2 Architecture Design

2.1 System Overview

A three layer architecture for accountability and privacy preservation is designed for the PHDM system. The data sharing layer provides users with entire control over their personal health data and handles data requests from third parties. The SGX enabled hardware layer provisions a trusted execution environment in the cloud, generates data access tokens and is responsible for reliable data storage and process. The blockchain network layer, which is distributed and untrusted, records data operations and various data access requests for immutability and integrity protection. Figure 1 is a general scenario for the patient centric personal health data management (PHDM) system. Personal wearable devices collect original health data, such as walking distance, sleeping conditions and heartbeat, which may be synchronized by the user with their online account associated with the cloud server and cloud database. Every piece of health data could be hashed and uploaded to the blockchain network for record keeping and integrity protection. The original data is maintained in the cloud database hosted on trusted platform enabled by SGX. The user owns personal health data, maintains access tokens and is responsible for granting, denying and revoking data access from any other parties requesting data access. For example, a user seeking

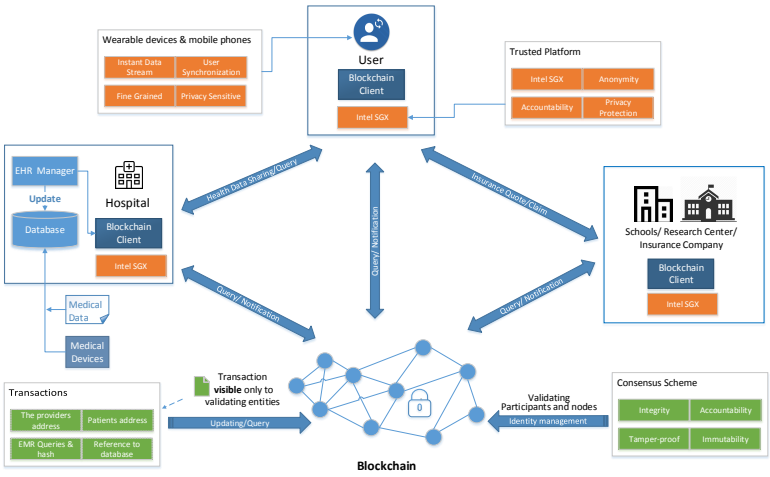


Fig. 1. Patient Centric Personal Health Data Management System Scenario.

medical treatment would grant the doctor a one time data access token. Same scenario applies to user-insurance company interactions. Besides, user can also manually record everyday activities according to a particular medical treatment such as medicine usage and share the information frequently with the doctor. Healthcare providers such as doctors can perform medical test, give suggestions or provide medical treatment, and request access to previous medical treatment from the patient. The data request and the corresponding data access is recorded on the blockchain for distributed validation. Besides, user may request a health insurance quote from insurance companies to choose health insurance plans. Insurance companies can also request access to user health data from wearable devices and medical treatment history. The blockchain network is used for three purposes. For health data collected from wearable devices and from healthcare providers, each of the hashed data entry is uploaded to the blockchain network for integrity protection. For personal health data access request from healthcare provider and health insurance company, a permission from the data owner is needed with a decentralized permission management scheme. Besides, each of the access request and access activity should be recorded on the blockchain for further auditing or investigation.

2.2 Key Establishment

In the patient centric data management system, users are required to register an online account to be involved in the system, and generate data encryption key pairs to encrypt their cloud data for confidentiality. For key management, we assume the system developers adopt a secure wallet service. The description of each key established is as follows.

- **User Registration Key** K_{UR}. The user needs to create an online account to store health data collected from wearable devices and other sources in the cloud database. We denote the user registration key as K_{UR}. Every time user wants to operate on their cloud health data, the registration key is needed. This key is generated from the platform identity key using Intel SGX anonymous key system and is thus bounded to the user. Even if the user's registration key is stolen or compromised, it could not be used elsewhere without the user authentication. Similarly, the registration key for healthcare provider and healthcare insurance company is K_{HR} and K_{IR}, respectively.
- **Data Encryption Key** K_{DE}. After registration, the user generates an encryption key K_{DE} to encrypt all the health data stored in the cloud database. When a health data entry is created, user has the option to encrypt the data entry, which limits the data access only to the key owners, and the hashed data entry will be uploaded instantly to the blockchain.
- **Data Sharing Public/Private Key Pair (PK_{DS}, PR_{DS})**. For health data sharing, a public/private key pair will be generated, denoted as (PK_{DS}, PR_{DS}). In some cases that the data sharing activity is to be recorded on the blockchain, the private key is used to generate a signature from the user to indicate the health data ownership, while the public key is used by others to verify the ownership. When users want to share their health data with healthcare providers or insurance companies, they share the private key for data access and the corresponding tokens generated with this private key.
- **Platform Identification Key** K_{PID}. Each trusted platform owns a platform identification key K_{PID}, also generated from the platform identity key using Intel SGX anonymous key system. Every health data request and data access on a certain platform will generate an activity record signed by K_{PID} for accountability while still with anonymity preserved. Different entity keys are noted as K_{PIDu} for users, K_{PIDp} for healthcare providers and K_{PIDi} for insurance companies.

2.3 PHDM Procedures

In the system, there are four phases for personal health data management including user registration, health data generation and synchronization (data generated from user, healthcare provider and insurance company), health data access management, health data access record uploading and health data access auditing.

User Registration. In the system, user needs to create an online account to store health data collected from wearable devices and other sources in the cloud database by way of establishing an online ID. Other entities in the system cannot correlate the online ID with their real identity, preserving user privacy in the registration phase.

Health Data Generation and Synchronization. Health data contains four categories, including data collected from wearable devices, data collected from medical test, data collected by patient indicating their treatment details and data recorded by healthcare providers and insurance companies. After registration, the user can collect health data from wearable devices, which monitor

their everyday activities, such as walking, bicycling and sleeping, and choose to synchronize those data with their online account. The collected data is encrypted using K_{DE} and stored in the cloud database. This preserves user privacy in the data generation and storage phase. The synchronization step triggers an event in the system which transforms the event into a transaction on the blockchain. Everytime a health data entry is created, user has the option to encrypt the data entry and upload the record on the blockchain.

Health Data Access Management. User can share data with healthcare providers to seek healthcare services, and with insurance companies to get a quote for the insurance policy and to be insured. A token based access control mechanism is adopted to control personal health data access and exposure. The health data is stored in the cloud database and the access control policies are stored on the blockchain in a decentralized way to ensure integrity and remove the necessity of a trusted third party. Both healthcare providers and insurance companies can request data access to the data owner, that is, the registered user in the system. User can grant, deny and revoke access from both parties. Each time there is a data request, the user will generate an Access Token to the requester. The Access Token is bound to a trusted platform for accountability.

Health Data Access Record Uploading. As mentioned above, once a data request or data access event is monitored in the system, the event will be captured as a data access record which will serve as a system log for future validation and regulation. The record is hashed and eventually transformed into a Merkle tree node [14] using Tierion API [4]. The Merkle tree root node will be anchored in a blockchain transaction following the Chainpoint 2.0 protocol [2]. For the blockchain nodes, both healthcare providers and insurance companies can join the blockchain mining process in exchange for the large-scale dataset retrieved from personal health database as mining rewards. For privacy concerns, the dataset removes sensitive information such as name and location and is anonymous. Insurance companies can learn more information from medical history and health data so that they can make specific policies according to the characteristics of customers. Healthcare providers can learn from previous medical treatment and gain experiences which will benefit future medical cases and improve medical levels.

Health Data Access Auditing. When it is necessary for legal regulators to investigate the system security, user can grant the system auditor access to the data records on blockchain network. Each data record is verifiable by checking the record signatures. It is also accountable against the trusted platform by identifying the platform key used in the signature.

3 Token-Based Access Control

For anonymity and verification purposes, we adopt the token based access control mechanism to handle the data management process. As is shown in Figure 2, the cloud server is responsible for issuing and verifying tokens, and also maintaining both the data record database and data access log database. Users can request

and share the access tokens to data requstors. Potential data requestors include healthcare providers, insurance companies and even system auditors. Each data and token operation is recorded in the blockchain and thus validated. After user registration, the cloud server can issue tokens based on the personal information provided by users. To access data, the required token will be presented to the cloud server and verified. The server issuance operation, the user token presentation and verification omit system logs which will be stored in the log database, as well as data requests and access from third parties.

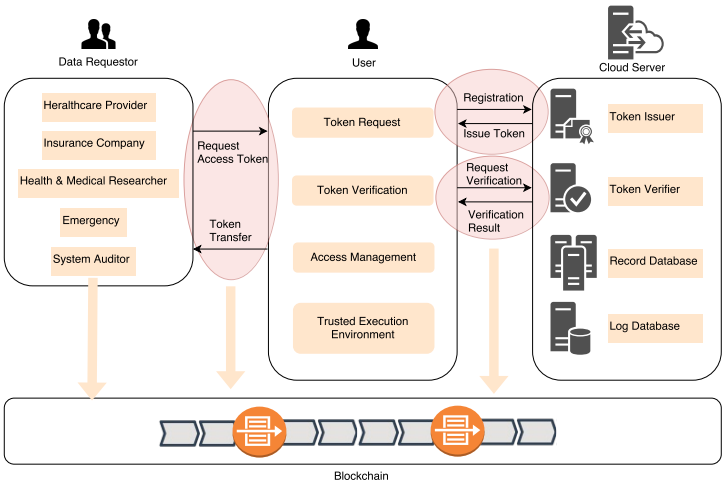


Fig. 2. PHDM System Interaction.

3.1 U-Prove Based Token Generation

User registration is based on U-Prove [17], which is proved capable to be integrated into Trusted Platform Module 2.0 in [6]. U-Prove [16] includes three entities, namely issuer, prover and verifier. In our system, the issuer and the verifier is the same entity, that is, the cloud server. The user in our PHDM system is the prover entity in U-Prove model. During user registration phase, there are some parameter definitions for both prover and issuer.

- The value of the token information field (TI): $TI \in (0,1)^*$
- The value of the prover information field (PI): $PI \in (0,1)^*$
- Application Attributes (AA): $(A_1, ..., A_n), TI$
  $(A_1, ..., A_n)$ indicates n attributes from the application itself.
- Issuer Parameters (IP): $UID_p, desc(G_p), UID_H, (g_0, g_1, ..., g_n, g_t), (e_1, ..., e_n), S$
  UID_p is an application-specific identifier for this particular IP, which is unique across the PHDM system and $desc(G_p)$ specifies the group (G_p) with

an order of p which is used for discrete logarithm computation in the following verification steps. UID_H is the identifier for the secure hash algorithm. $(g_0, g_1, ..., g_n, g_t)$ is the Issuer's public key. $(e_1, ..., e_n)$ is generated from AA, indicating the format of each application attribute.
- The hash of the $IP(P)$: $P = H(IP)$
- Device-protected Boolean (DB): d
  This indicates whether the protocol is device protected. PHDM adopts trusted execution environment so the value by default is $true$.
- Device Parameters (DP): g_d, x_d, h_d
  The Device generator g_d satisfies $g_d \in G_q$. x_d is device private key and h_d is the public key.

With the above information provided, we choose the issuance protocol version number 0x01. The user platform identification key K_{PIDu} is used to generate the device private key. The token generation protocol is as follows.

Protocol 1 User Registration on the Cloud Server

Input:
$x_t = Hash(0x01, P, TI)$, $x_i = Hash(A_i)$, $\gamma = g_0 g_1^{x_1} ... g_n^{x_n} h_d$
UID_p, random $\alpha, \beta_1, \beta_2, \omega$, and issuer private key y_0

Compute:
$h = \gamma^{\alpha}$, $\sigma_z = \gamma^{y_0}$, $\sigma_z^1 = \gamma^{y_0}$, $\sigma_a^1 = g_0^{\beta_1} g^{\beta_2} g^{\omega}$, $\sigma_b^1 = (\sigma_z^1)^{\beta_1} h^{\beta_2} \gamma^{\omega\alpha}$
$\sigma_c^1 = Hash(h, PI, \sigma_z^1, \sigma_a^1, \sigma_b^1)$, $\sigma_r^1 = (\sigma_c^1 + \beta_1 \mod q) y_0 + \omega \mod q + \beta_2 \mod q$

Output:
U-Prove token T: UID_P, h, TI, PI, σ_z^1, σ_c^1, σ_r^1, d
prover private key: α^{-1}

The cloud server issues tokens to users with the signature $(\sigma_z^1, \sigma_c^1, \sigma_r^1)$. For privacy concerns, the application attributes are hashed for the generation of U-Prove based token. During some circumstances, the issuer is able to generate multiple tokens at one time for better performance.

3.2 Token Presentation Protocol

A presentation proof of ownership of certain messages or attributes contained in the token is generated using the token private key and is required to access user data in the cloud database. Before accessing data, the data requestor needs to attest itself and convince the user that it is running on top of SGX enabled environment in an isolated enclave. The SGX attestation is launched by the data requestor which will send a signed quote to the data owner for verification using the platform dependent key. The remote attestation between the two platforms is performed with the assistance of the Intel Attestation Service [5]. After the verification, the user will request a one-time U-Prove token with a newly generated private key PR_{DS} and share it with the data requestor. The data requestor

forwards the token to the verifier of the cloud database and will be granted access after the verification. Different decisions can be made by the user, such as to grant, deny and revoke access. The presentation proof serves two purposes. For one thing, it proves the integrity and the authenticity of the attribute values and for another, it establishes the confirmation of the ownership of the private key associated with the token itself, which will further prevent token replay attack.

4 Decentralized Accountability and Integrity Protection

As is shown in Figure 2, each data and token operation is recorded in the blockchain and thus validated in a decentralized and permanent manner, ensuring data integrity. Besides, every operation is launched on a trusted platform enabled by Intel SGX, making the operation record trustworthy and nonframeable. The event record can be described using a tuple as {*datahash, owner, receiver, time, location, expirydate, signature*} where the signature comes with platform dependency for accountability. Then the tuple is submitted to the blockchain network which is followed by several steps to transform a list of records into a transaction. A list of transactions will be used to form a block, and the block will be validated by nodes in the blockchain network by consensus algorithms. After a series of processes, the integrity of the record can be preserved, and future validation on the block and the transaction related to this record is accessible. Each time there is an operation on the personal health data, a record will be reflected and anchored to the blockchain. The SGX platform identification key K_{PID} is used to generate the signature thus making each record platform dependent and ensuring that every action on personal health data is accountable. The token generation and issuance are also recorded in the same way so as to track the data requests and authorizations.

For scalability considerations, we adopt a Merkle tree based architecture [15] to handle large number of data records. Each leaf node represents a record and the intermediate node is computed as the hash of the two leaf nodes. The Merkle root, along with the tree path from the current node to the root, serves as the proof of integrity and validation, that is, the Merkle proof. The basic Merkle proof is shown in Figure 3. First, we need to identify the record location, the targetHashB. The target hash and the path to the Merkle root, that is, nodes in green, constitute the Merkle proof of the hashed data record, which is stored in a JSON-LD document that contains the information to cryptographically verify that the record is anchored to a blockchain. By calculating the hashes in different tree levels, it is easy and fast to obtain the root hash, which is anchored in the blockchain transaction, witnessed and maintained by some distributed nodes. It proves the data was created as it was at the time anchored. The Merkle root for each Merkle tree is related to one transaction in the blockchain network, which means a blockchain transaction represents a list of data records the Merkle hosts, enabling the scalability and effectiveness of data integrity protection and validation. The tree based architecture protects the integrity of each operation record itself which can be validated by traversing the tree nodes. Meanwhile, it implic-

itly indicates the integrity of all the nodes in that any single node modification could lead to the modification of the root, thus protecting the integrity of the whole tree structure at trivial costs.

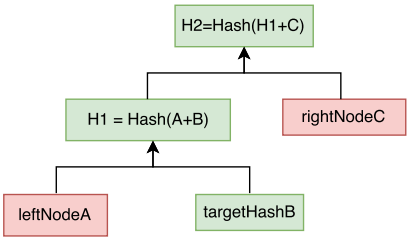


Fig. 3. Merkle Tree Based Data Integrity Protection.

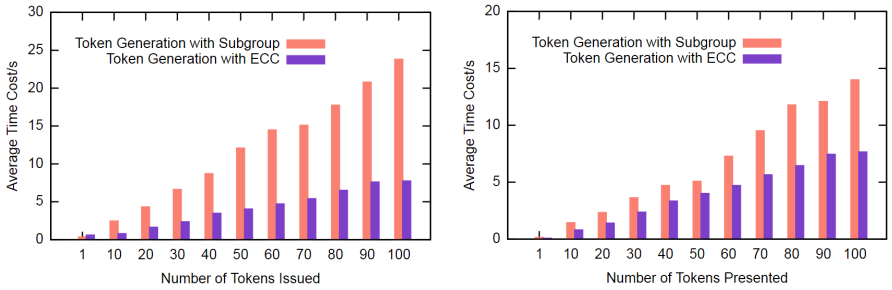
5 System Evaluation

To evaluate the performance of the system and overhead brought by the security measures, we adopt two metrics, including the efficiency to handle different number of accountable records and generate large numbers of tokens. For record anchoring, the tree based algorithm bears a computation complexity of $log(n)$ and the average time cost for each record is 0.4 ms when 1000 entries are processed concurrently.

For U-Prove based token generation, we select five attributes predefined and involved in each token and two of them are required to obtain a data access token. During the token issuance, there are basically two cryptographic methods for digital signature including Subgroup and ECC. The evaluation results for token issuance and presentation with these two methods are shown in Figure 4(a) and Figure 4(b). It can be concluded that ECC-based token generation is more efficient than the subgroup-based method. This can be explained that ECC utilizes shorter key length for the elliptic curve than subgroups of equivalent security levels and computes faster with a small field. Adopting the ECC-based U-Prove protocols for both token issuance and presentation, the average overhead brought to the system is 8.1% and 9.4%, respectively.

6 Conclusion and Future Work

Some work [18] has been done to integrate blockchain technology to the healthcare industry. MedRec [8] is proposed to build the healthcare on top of smart contract. But still, privacy risks remain to be addressed. [21] points out that MPC (Secure Multi-Party Computing) is a promising solution to enable untrusted third-party to conduct computation over patient data without violating privacy but the actual efficiency is not clear. [22] addresses the adoption of blockchain



(a) Average Time for Token Issuance (b) Average Time for Token Presentation

Fig. 4. Average Time Cost for Token Issuance and Presentation

in social network domain but not fully explores the benefits of the blockchain. [11] addresses the blockchain adoption in Internet of Things environment.

In this paper, we build a web based system for personal health data management using blockchain and Intel SGX. By utilizing blockchain technology in the self-sovereign healthcare systems, we manage to distribute the responsibility of maintaining trusted records for data operation as well as token generations. Meanwhile, benefiting from the blockchain consensus scheme and the decentralized architecture, along with the trusted execution environment and the platform dependency provisioned by Intel SGX, the records are anchored with trusted timestamping and redundancy, preserving both availability and accountability of the healthcare data and operations. We also propose a U-Prove based protocols for the permission management. We implement a prototype of the PHDM system and the evaluation shows that the performance is acceptable. In the future, we will integrate the PHDM system with the enhancement of a blockchain based access control scheme to provide better data protection and user privacy.

7 Acknowledgements

This work was supported by Office of the Assistant Secretary of Defense for Research and Engineering (OASD (R& E)) agreement FA8750-15-2-0120. The work was also supported by a grant from the National Natural Science Foundation of China (No.61402470) and the research project of Trusted Internet Identity Management (2016YFB0800505 and 2016YFB0800501).

References

1. 2016 connected patient report, `https://www.salesforce.com/assets/pdf/industries/2016-state-of-the-connected-patient-pr.pdf`
2. Chainpoint: A scalable protocol for anchoring data in the blockchain and generating blockchain receipts, `http://www.chainpoint.org/`

3. Insurance 3.0 - The Turn of the Digital. http://www.huxley.com/fr/actualites-et-articles-de-fond/actualites/insurance-3-0-le-virage-du-digital, [Online; accessed 7-March-2017]
4. Tierion api, https://tierion.com/app/api
5. Anati, I., Gueron, S., Johnson, S., Scarlata, V.: Innovative technology for cpu based attestation and sealing. In: Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy. vol. 13 (2013)
6. Chen, L., Li, J.: Flexible and scalable digital signatures in tpm 2.0. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. pp. 37–48. CCS '13, ACM, New York, NY, USA (2013), http://doi.acm.org/10.1145/2508859.2516729
7. Clippinger, J.H.: Why Self-Sovereignty Matters. https://idcubed.org/chapter-2-self-sovereignty-matters/, [Online; accessed 7-March-2017]
8. Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A.: A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference (2016)
9. Hardjono, T., Pentland, A.S.: Verifiable anonymous identities and access control in permissioned blockchains
10. Kish, L.J., Topol, E.J.: Unpatients-why patients should own their medical data. Nature biotechnology 33(9), 921–924 (2015)
11. Liang, Xueping Zhao, J., Shetty, S., Li, D.: Towards data assurance and resilience in iot using distributed ledger. In: IEEE Milcom. IEEE (2017)
12. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L.: Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: International Symposium on Cluster, Cloud and Grid Computing. IEEE/ACM (2017)
13. Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications (10 2017)
14. Merkle, R.C.: Protocols for public key cryptosystems. In: Security and Privacy, 1980 IEEE Symposium on. pp. 122–122 (April 1980)
15. Merkle, R.C.: Protocols for public key cryptosystems. In: Security and Privacy, 1980 IEEE Symposium on. pp. 122–122. IEEE (1980)
16. Paquin, C.: U-prove technology overview v1.1 (revision 2) (April 2013), https://www.microsoft.com/en-us/research/publication/u-prove-technology-overview-v1-1-revision-2/
17. Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1. 1. Technical Report, Microsoft Corporation (2011)
18. Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K.: A blockchain-based approach to health information exchange networks (2016)
19. Sarangdhar, N., Nemiroff, D., Smith, N., Brickell, E., Li, J.: Trusted platform module certification and attestation utilizing an anonymous key system (May 19 2016), https://www.google.com/patents/US20160142212, uS Patent App. 14/542,491
20. Thierer, A.D.: The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Richmond Journal of Law & Technology 21, 1 (2014)
21. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems 40(10), 218 (Aug 2016), https://doi.org/10.1007/s10916-016-0574-6
22. Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. IEEE Access 4, 9239–9250 (2016)