USING BLOCKCHAIN TO ACHIEVE DECENTRALIZED PRIVACY IN IOT HEALTHCARE

Sajad Meisami[1], Mohammad Beheshti-Atashgah[2]
and Mohammad Reza Aref[2]

[1]Department of Computer Science, Illinois Institute of Technology, Chicago, USA
[2]Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran

ABSTRACT

With the advent of the Internet of Things (IoT), e-health has become one of the main topics of research. Due to the sensitivity of patient information, patient privacy seems challenging. Nowadays, patient data is usually stored in the cloud in healthcare programs, making it difficult for users to have enough control over their data. The recent increment in announced cases of security and surveillance breaches compromising patients' privacy call into question the conventional model, in which third-parties gather and control immense amounts of patients' Healthcare data. In this work, we try to resolve the issues mentioned above by using blockchain technology. We propose a blockchain-based protocol suitable for e-health applications that does not require trust in a third party and provides an efficient privacy-preserving access control mechanism. Transactions in our proposed system, unlike Bitcoin, are not entirely financial, and we do not use conventional methods for consensus operations in blockchain like Proof of Work (PoW). It is not suitable for IoT applications because IoT devices have resources-constraints. Usage of appropriate consensus method helps us to increase network security and efficiency, as well as reducing network cost, i.e., bandwidth and processor usage. Finally, we provide security and privacy analysis of our proposed protocol.

KEYWORDS

Blockchain, Healthcare, IoT, Privacy, E-Health, Access Control, Security

1. INTRODUCTION

Many societies in the world are facing a significant increase in the number of medical patients, and access to primary doctors or medical staff is becoming more difficult for patients. Internet of Things (IoT) allows any device to connect to other devices and the Internet at any time and any place, and researchers hope that more than 75 billion devices will be able to connect to the Internet by 2025 [1]. Fortunately, e-health is one of the main applications of IoT, and it can help medical staff be able to treat more patients and provide more comfort and convenience for patients. Patients can stay connected with medical staff as required. It also reduces medical costs and improves the quality of care and treatment.

In recent years, the improvement of the IoT has allowed us to use electronic wearable devices to implement e-health. Wearable devices measure a patient's vital signs like heart rate, blood glucose, body temperature, blood pressure, etc. These wearable devices automatically collect patient health data and transfer it to central storage or cloud for further processing by medical staff to facilitate health monitoring, disease diagnosis, and treatment [2].

David C. Wyld et al. (Eds): DBML, CITE, IOTBC, EDUPAN, NLPAI -2023
pp. 97-108, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120208

Patients' healthcare data are highly privacy-sensitive and sharing of data may raise the risk of exposure. These data usually stored on a server and processed remotely, and this raises concerns regarding the privacy and confidentiality of patients' healthcare data. Also, several security attacks are possible in such cases; for example, an attacker can track patients' data on the Internet and modify or replace it with incorrect data in the data center, or an attacker can steal information from remote servers [3].

1.1. Organization

Section II describes the related work involved. Section III discusses the challenges we solve in this paper. Sections IV provides an overview of the system model, whereas section V explains the network protocol in detail. Section VI discusses the security and privacy of the proposed model, and section VII provides a conclusion.

2. RELATED WORKS

To address the privacy issue on personal data, researchers developed various methods. One of them is data anonymization that attempts to protect personally identifiable information. For example, in the k-anonymity method used in anonymous datasets, any necessary recorded data is indistinguishable from at least k−1 other important recorded data [4]. However, in recent research, it has been shown, anonymized datasets can be broken even with a little information (their anonymity disappears) [5]. There exist other privacy-preserving methods like differential privacy, that perturbs data, or adds noise to the computational process before sharing the data [6] and practices on creating noisy data or summarizing [7]. These methods are not efficient in healthcare applications where patients' original data are required to send to medical staff for medical treatments.

Attribute-based encryption (ABE) is a useful technology that can provide data privacy and fine-grained access control when users want to secretly share data stored in a third-party cloud server [8]. Almost all ABE schemes require a trusted private key generator (PKG) to set up the system and distribute for users the corresponding secret key [9]. However, in all ABE schemes, the PKG can decrypt all data stored in the cloud server, which may cause serious problems such as privacy data leakage and key abuse. Furthermore, the traditional cloud storage model runs in a centralized storage manner, so existence a single point of failure can collapse the system. Other encryption schemes exist that allow running computations and queries over encrypted data that called fully homomorphic encryption (FHE) [10] but are currently too unsuitable to use in practice widely.

In recent years, decentralized cryptocurrency systems have emerged. Bitcoin was the first of these systems, which use blockchain technology. Bitcoin allows users securely to make transactions and transfer currency (bitcoins) with others without the need to trusted third-party [11]. Blockchain works as an immutable timestamp ledger of blocks that are shared across all participating nodes in the network, which can bypass the need for a central authority [12]. This technology is used for sharing and storing data in a distributed manner by a peer-to-peer network [13]. Nowadays, blockchain is playing an effective role in financial transactions [14]. Also, it can be a facilitator in many other fields. Such as decentralized IoT [15], identity-based PKI [16], decentralized supply chain [17], decentralized proof of document existence [18], decentralized storage [19–21], etc.

In [22], the work by Zyskind et al. has shown the use of blockchain technology to construct an access control and management platform for personal data. They focused on users' privacy. And they combine blockchain and off-chain storage to storing encrypted data out of blockchain ledger

while pointers to the encrypted data exist on the blockchain. Recently researchers addressed the security and privacy issues on healthcare data, using blockchain technology, and proposed new schemes [23–26].
In this paper, we combine IoT and blockchain technology to construct a novel platform for patients' healthcare data management that satisfies privacy and security requirements.

3. CHALLENGES AND OUR SOLUTIONS

Secure transmission and preservation of privacy for the patients' healthcare data are the main concerns in the e-health application of IoT. However, the decentralized essence of the blockchain and other attributes like immutability and transparency make blockchain very suitable for e-health. But there are still challenges for applying blockchain into the IoT. Now we discuss the challenges and explain our solutions.

3.1. Scalability

IoT devices are resource-restricted, so it's hard for them to solve computationally intensive problems to execute a consensus algorithm for adding a new blocks to the blockchain ledger, especially in Proof-of-Works (PoW). We eliminate the concept of PoW for consensus in our blockchain network and use a method called Practical Byzantine Fault Tolerance (PBFT), a consensus method based on voting [27]. BPFT involves multiple rounds of voting by all nodes of the network [28]. BPFT helps us to reduce network costs, i.e., bandwidth, need for processors, and energy for consensus operations.

3.2. Data Storage

It's not practical and suitable to store IoT big data on the blockchain ledger. Because of this, we do not store the data on the blockchain, but only we store the pointers to the data (hash of encrypted data) on blockchain to lighten the storage space of blockchain. The data (encrypted data) are stored on Off-chain storage (see section IV, E. Off-chain Storage).

3.3. Security of Data

Patients' healthcare data are highly sensitive. To satisfy the security of data, we use a symmetric key encryption scheme (see section V, A. Cryptographic Techniques Used in The System). At first, The data is encrypted by symmetric key encryption and then sent to the blockchain network. So even in Off-chain Storage, the information is stored in the form of encrypted data.

3.4. Patients' Privacy

The main concern that is addressed in this paper is preserving patients' privacy because Patients' healthcare data is highly privacy-sensitive. We assume that the medical staff is honest-but-curious (i.e., they follow the protocol). In our system, patients could be remain (pseudo) anonymous. At the same time, medical staff profiles could be stored on the blockchain so that patients can trust medical staff by verifying medical staff identities. Our proposed platform satisfies the following Items:

1) Patients' Data Ownership: In our platform, patients are the only owner of their healthcare data, and only they can control that data. As such, the platform recognizes the medical staff as Service Providers with granted permissions set and the patients as healthcare data owners.

2) Fine-grained Access Control: Each patient can grant a set of permissions to Any desired member of the medical staff for accessing a patient's healthcare data. Also, the patient can alter or revoke the set of granted access permissions. These permissions are securely stored on blockchain ledger as access-control policies, where only the patient can change or revoke them.
3) Data Transparency and Auditability: Patients have complete and Accurate transparency over their collected healthcare data, and they can know how medical staff can access to healthcare data.

4. OUR SYSTEM MODEL

As demonstrated in Figure 1, our proposed system model consists of the following main modules:

1) Wearable IoT devices.
2) Patient's smartphone.
3) Medical staff.
4) Blockchain.
5) Off-chain storage.

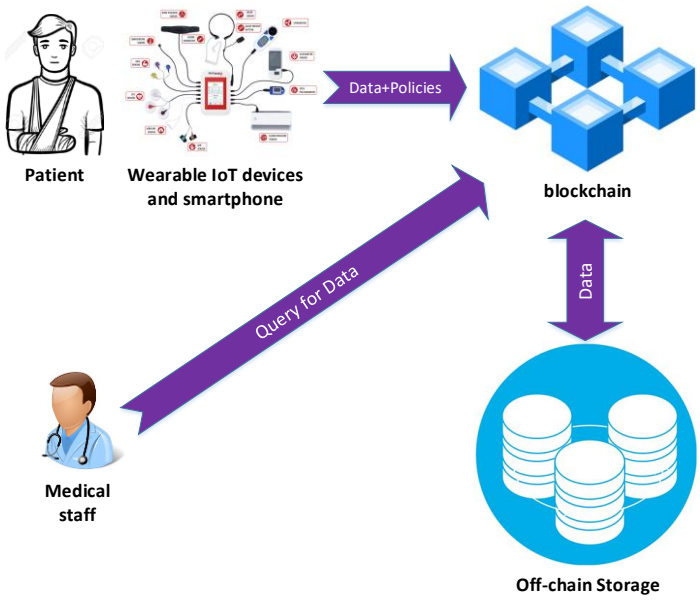

Fig. 1. Our proposed system model.

4.1. Wearable IoT devices

The wearable IoT devices will collect all healthcare data from the patient's body, such as blood pressure, body temperature, and heart rate. These devices have limitations in resources such as low energy, low processing power, and little storage space. By considering these limitations, wearable IoT devices send the collected healthcare data to the patient's smartphone using short-range communication, such as Bluetooth or Zigbee.

4.2. Patient's Smartphone

Smartphones are more potent than IoT devices because smartphones have more storing space, more battery life, and higher processing power. So smartphones can do more complicated works,

such as computational and cryptographic operations. Also, smartphones can transmit data via long-range communications (such as cellular networks) that can play the role of a gateway and allow patients to interact with the blockchain network.

4.3. Medical Staff

Medical staff, including physicians and nurses, should receive patients' healthcare data and, after analyzing it, obtain information about the patient's health status. Then they provide appropriate treatment for patients.

4.4. Blockchain

In our work, we use blockchain to store access policies and eliminate the need for a third-party that preserves network against DoS attack and single point of failure. It also ensures the availability and integrity of the patients' data.

The data is not stored on the blockchain, but only the pointers to the data (hash of encrypted data) are stored on it to lighten the storage space of blockchain. Also, because the use of PoW in IoT applications is not appropriate, we use PBFT for consensus operations.

4.5. Off-Chain Storage

We store patients' encrypted data on off-chain storage. For the implementation of off-chain storage, we use The InterPlanetary File System (IPFS) [21] that is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. It provides a high throughput content-addressed block storage model, with content-addressed hyperlinks. IPFS combines a distributed hashtable (or DHT), an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other [21]. In IPFS, we distribute the data and store them on different servers all over the world. Not using the central server is the reason for the advantage of IPFS over conventional cloud storage.

5. THE NETWORK PROTOCOL

In this section, we describe the protocol used in our system in detail.

5.1. Cryptographic Techniques used in the System

Hash Function: We use SHA-256 [29] to implement the hash function (H indicates the hash function).

Symmetric Key Encryption: Symmetric algorithm uses the same key for encryption of plaintext and decryption of ciphertext. We use AES [30] to implement the symmetric key encryption (G_{enc} indicates generating algorithm).

Digital Signature Scheme: Digital signature is added to the data for authentication purposes. For the implementation of the digital signature, we use ECDSA with a secp256k1 curve [31] (G_{sig} indicates generating algorithm).

5.2. Protocol in Detail

staff *m* each generates a pair of private and public keys to sign and send transactions to the blockchain network and announce their public key (as their address) on the network. Patient *P* also generates a secret key for encrypting data with an AES symmetric encryption algorithm. Then the patient shares the secret key with the chosen member of the medical staff so that, later, she will be able to decrypt her authorized data with that secret key.

Protocol 1 Joining the Blockchain

1: **procedure** GENERATING(*p,m*)
2: *p executes:*
3: $(pk^{p}_{sig}, sk^{p}_{sig}) \leftarrow G_{sig}( )$
4: $sk^{p,m}_{enc} \leftarrow G_{enc}( )$
5: *p shares* pk^{p}_{sig} *(as address) on the network*
6: *m executes:*
7: $(pk^{m}_{sig}, sk^{m}_{sig}) \leftarrow G_{sig}( )$
8: *m shares* pk^{m}_{sig} *(as address) on the network*
9: *p shares* $sk^{p,m}_{enc}$ *with m from secure channel*
10: // Both *p* and *m* have $sk^{p,m}_{enc}$
11: **return** $pk^{p}_{sig}, pk^{m}_{sig}, sk^{p,m}_{enc}$
12: **end procedure**

Registration of access policy: We denote the data access permissions by $POLICY_{p,m}$, which indicates the permissions that the patient *p* gives to the selected member of the medical staff *m* so that she can access a particular type or all of the patient's data. For example, $POLICY_{p,m}$ = *{body temperature, blood pressure}*.

Protocol 2 Access Control Transaction

1: **procedure** ACCESSTX(pk^{k}_{sig} ,*message*)
2: $s \leftarrow 0$
3: $(pk^{p}_{sig} \,||\, pk^{m}_{sig} \,||\, POLICY_{p,m}) = message$
4: **if** $pk^{k}_{sig} = pk^{p}_{sig}$ **then**
5: $L[H(pk^{k}_{sig})] \leftarrow L[H(pk^{k}_{sig})] \cup message$
6: *// L is Blockchain memory*
7: $s \leftarrow 1$
8: **end if**
9: **return** *s*
10: **end procedure**

By sending a T_{access} transaction on the blockchain network that contains $POLICY_{p,m}$, the patient gives the desired permissions to the medical staff. As illustrated in protocol 2, this transaction is performed in the nodes of the blockchain, and it is checked the patient himself has sent the transaction, then the set of permissions are stored on the blockchain ledger.

The patient can send new T_{access} transactions and change the permissions set granted to the medical staff. Also, Sending the empty set by the patient can revoke all access-permissions set previously granted.

Data storage and retrieval: T_{data} transaction is used to store patients' encrypted healthcare data on off-chain storage (IPFS) or access stored data and receive it. The patient (to store and retrieve the

data) and the medical staff (only to retrieve the data) can send the T_{data} transaction to the blockchain network.

If the T_{data} transaction (by the patient or the medical staff) is sent to the network, the nodes in the blockchain first check with the following protocol (protocol3) whether they have access permissions or not?

Protocol 3 Blockchain Permissions Checking

1: **procedure** POLICYCHECK(pk^k_{sig} ,*T*) *//T=type of data*
2: $s \leftarrow 0$
3: **if** $L[H(pk^k_{sig})] \neq \emptyset$ **then**
4: $(pk^p_{sig} \,||\, pk^m_{sig} \,||\, POLICY_{p,m}) \leftarrow L[H(pk^k_{sig})]$
5: **if** $pk^k_{sig}=pk^p_{sig}$ **or**
6: $(pk^k_{sig}=pk^m_{sig}$ *and* $T \in POLICY_{p,m})$ **then**
7: $s \leftarrow 1$
8: **end if**
9: **end if**
10: **return** *s*
11: **end procedure**

Now, after checking the access permissions and the transaction sender's approval, he or she can store or retrieve patients' encrypted healthcare data with the following protocol.

Protocol 4 Data Transaction

1: **procedure** DATATX(pk^k_{sig} ,*message*)
2: $(C \,||\, T \,||\, RW) = message$
3: *// C=encrypted data , T=type of data*
4: *//RW=read data*(=1) or write data(=0)
5: **if** POLICYCHECK(pk^k_{sig}, T)=True **then**
6: $(pk^p_{sig} \,||\, pk^m_{sig} \,||\, POLICY_{p,m}) \leftarrow L[H(pk^k_{sig})]$
7: **if** $RW = 0$ **then**
8: $L[pk^k_{sig} \,||\, T] \leftarrow L[pk^k_{sig} \,||\, T] \cup H(C)$
9: *(IPFS)* $ds[H(C)] \leftarrow C$
10: **return** $H(C)$
11: **else if** $C \in L[pk^k_{sig} \,||\, T]$ **then**
12: (*IPFS*) **return** $ds[H(C)]$
13: **end if**
14: **end if**
15: **return** ∅
16: **end procedure**

Note that we used *IPFS* shorthand notation in lines 9 and 12 of Protocol 4 for accessing the off-chain storage. *IPFS* instruction cause to send Off-blockchain network message in off-chain storage for storing or retrieving data.

With the above protocols, the patient can easily upload the encrypted healthcare data in the network. The chosen members of the medical staff can also receive the encrypted data if there is a permission, and then with the $sk^{p,m}_{enc}$ that they have received before (in protocol 1), they can decrypt encrypted data and access the original healthcare data.

6. SECURITY AND PRIVACY ANALYSIS

In this section, we discuss and investigate the performance of our proposed protocol in terms of security and privacy. For security designing in any model, there are exist three main security requirements that need to be addressed: Confidentiality, Integrity, and Availability, known as CIA [32]. Confidentiality makes sure that the system's messages should be read by only authorized users who can access the system. The data integrity is responsible for making sure that no one without permission can change the stored data, and the availability of the data means that when users needed to the data, it is available to them. Now, we summarize the aforementioned primary security requirement evaluation in Table 1.

Table 1. Security Requirement Analysis.

Requirement	Model Solution
Confidentiality	Achieved by using symmetric key encryption.
Integrity	Hashing of data blocks in blockchain is employed to achieve integrity.
Availability	Achieved by limiting acceptable transactions in the network.
Authorization	Using digital signature to achieve authorization.

In our model, data ownership is emphasized for preserving privacy. That means only the patients (users) can control their data. The decentralized nature of the blockchain technology and using digital-signature to sign transactions in the network ensure that an adversary cannot be able to infiltrate the system as a user. Because gaining control over the majority of the network's resources (at least 51%), or forging digital-signature is almost impossible for the adversary. Also, the model ensures other privacy-preserving parameters that we previously mentioned (in section III) like, Data Transparency and Auditability. Fine-grained access control is satisfied by storing access-control policies on a blockchain ledger, where only the patient can change or revoke them. In Table 2, we have made a comparison between our proposed model and other existing systems. We considered a few attacks and analyzed the resilience of our model against each of them in Table 3.

Table 2. Comparison of Different Existing Systems.

Model Name / Property	Yang[33]	Xia-I[34]	Xia-II[35]	Peterson[36]	Zang[37]	A.Zhang[38]	Our Proposed Model
Access control	✓	✓	✓	✓	✓	✓	✓
Blockchain-Based	×	✓	✓	✓	×	✓	✓
Privacy Preserving	✓	✓	✓	✓	✓	✓	✓
IPFS Off-chain storage	×	×	×	×	×	×	✓

Table 3. Security Analysis Against Attacks

Attack	**Definition**	**Defence**	**Resilience**
Denial of Service (DOS) Attack	Attacker generates a large number of transactions to increase traffic in the network and disrupt the blockchain.	Only two types of transactions can be sent in the network. Also, each node can send a limited number of transactions, and the blockchain network will reject the rest of the user's transactions after receiving a few messages from a specific node.	High
Modification Attack	Attacker modifies or removes the stored patients' data (like access policies and hash) on the blockchain ledger.	Blockchain uses an immutable ledger.	High
Public blockchain Modification	Attacker advertises a false ledger of blocks and makes it as the longest ledger.	We use the private type of blockchain, so the nodes are from outside the organization cannot work as miners to create a malicious block.	High
Storage Attack	Attacker wants to remove, change, or add data in the Off-chain storage.	On blockchain ledger exist a hash of the encrypted data stored in the Off-chain storage; therefore, changes in the data can easily be detected.	High
Appending Attack	Attacker compromises a miner and generates blocks with fake transactions to create a false reputation.	Due to the usage of private blockchain, so the users cannot generate a fake block, whereas miners in the blockchain must verify any transaction.	High
51% Attack	Attacker controls more than 51% of miners and tries to compromise the consensus	The probability of occurrence of this attack is very low due to the	High

	algorithm and generate a fake block.	usage of private blockchain and PBFT method for consensus.	
Distributed DOS (DDOS) Attack	This is a distributed version of the Denial of Service (DOS) Attack.	A valid node can send a limited number of transactions in the network. After the blockchain network receives a transaction, miners check that received transaction has produced by a valid node then accept it.	Moderate

7. CONCLUSION

Patients' healthcare data are privacy-sensitive and security-sensitive, and for managing them, we should not trust in the third-parties, where they are vulnerable to attacks and abuse. In this work, we proposed a novel platform based on the Internet of Things (IoT) and blockchain technology, motivated by the privacy and security challenges of patients' healthcare data in e-health. Our proposed platform enables patients to have ownership and full control over their sensitive healthcare data collected by their IoT wearable devices. This ownership and complete control over patients' data are satisfied by storing access control policies in a blockchain ledger by patients to specify who from medical staff can access patients' data. In this platform, we use off-blockchain storage to lightening the blockchain storage. Also, we use a suitable consensus method in the blockchain network due to the resource constraint factor of IoT.

ACKNOWLEDGEMENT

The authors are thankful to Mr. Mohammad Doost and Mr. Mohammadhadi Ahmadiashtiyani for consulting and lengthy discussions on many of the ideas used in this paper.

REFERENCES

[1] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of connected-devices-worldwide/

[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678 - 708, June 2015.

[3] K. Abouelmehdi, A. Beni-Hessane and H. Khaloufi, "Big healthcare data preserving security and privacy," Journal of Big Data, December 2018.

[4] Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557–570, 2002.

[5] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105, 2006.

[6] Cynthia Dwork. Differential privacy. In Automata, languages and programming, pages 1–12. Springer, 2006.

[7] Y.-A. d. Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland "Protecting the Privacy of Metadata through SafeAnswers," PLOS ONE vol. 9, July 2014.

[8] A.Sahai and B.Waters, ‘‘Fuzzy identity-based encryption,’’ in Proc.Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 2005, pp. 457–473.

[9] J. Zhang, X. A. Wang, and J. Ma, ‘‘Data owner based attribute based encryption,’’ in Proc. Int. Conf. Intell. Netw. Collaborative Syst. (INCOS), Sep. 2015, pp. 144–148.

[10] Craig Gentry. Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 169–178, 2009.
[11] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008.
[12] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy, arXiv:1712.02969 , Dec 2017.
[13] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smar Contracts," in 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, August 2016.
[14] Blockchain for Financial Services. Accessed: Mar. 25, 2018. [Online]. Available: https://www.ibm.com/blockchain/financial-services
[15] A Decentralized Network for Internet of Things. Accessed: Mar. 25, 2018. [Online]. Available: https://iotex.io
[16] C. Fromknecht and D. Velicanu. (2014). A Decentralized Public Key Infrastructure With Identity Retention. [Online]. Available: https://eprint.iacr.org/2014/803.pdf
[17] Blockchain for Supply Chain. Accessed: Mar. 25, 2018. [Online]. Available: https://www.ibm.com/blockchain/supply-chain
[18] Proof of Existence. Accessed: Mar. 25, 2018. [Online]. Available: https://proofofexistence.com
[19] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, ‘‘Storj a peerto-peer cloud storage network,’’ White Paper. Accessed: Mar. 25, 2018. [Online]. Available: https://storj.io/storj.pdf
[20] P. Labs. (2018). Filecoin: A Decentralized Storage Network. [Online]. Available: https://filecoin.io/filecoin.pdf
[21] J. Benet. (2014). ‘‘IPFS-content addressed, versioned, P2P file system.’’ [Online]. Available: https://arxiv.org/abs/1407.3561
[22] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In 2015 IEEE Security and Privacy Workshops, pp. 180-184. IEEE, 2015.
[23] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized Privacy Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks," arXiv:1802.01746, Feb 2018.
[24] Fan, Kai, Shangyang Wang, Yanhui Ren, Hui Li, and Yintang Yang. "Medblock: Efficient and secure medical data sharing via blockchain." Journal of medical systems 42, no. 8 (2018): 136.
[25] X. Yue, H. Wang, D. Jin, M. Li and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Nove Privacy Risk Control," Journal of Medical Systems, 2016.
[26] Dwivedi, Ashutosh Dhar, Gautam Srivastava, Shalini Dhar, and Rajani Singh. "A decentralized privacy-preserving healthcare blockchain for IoT." Sensors 19, no. 2 (2019): 326.
[27] M. Castro, B. Liskov et al., “Practical byzantine fault tolerance,” in OSDI, vol. 99, 1999, pp. 173–186.
[28] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and a. M. H Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," IEEE Communications Society, 2018.
[29] Federal Information and Processing Standards. FIPS PUB 180-4 Secure Hash Standard (SHS). (March), 2012.
[30] Daemen, Joan, and Vincent Rijmen. The design of Rijndael. Vol. 2. New York: Springer-verlag, 2002.
[31] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). International Journal of Information Security, 1(1):36–63, 2001.
[32] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.
[33] Y. Yang and M. Ma, “Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 4, pp. 746–759, 2015.
[34] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, “Bbds: Blockchain-based data sharing for electronic medical records in cloud environments,” Information, vol. 8, no. 2, p. 44, 2017.
[35] Doost, M., Alireza Kavousi, J. Mohajeri and M. Salmasizadeh. “Analysis and Improvement of an E-voting System Based on Blockchain.” 2020 28th Iranian Conference on Electrical Engineering (ICEE) (2020): 1-4.

[36] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14757–14767, 2017.
[37] Khalesi, Ali, Mahtab Mirmohseni, and Mohammad Ali Maddah-Ali. "The Capacity Region of Distributed Multi-User Secret Sharing." arXiv preprint arXiv:2103.01568 (2021).
[38] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A blockchain-based approach to health information exchange networks,” in Proc. NIST Workshop Blockchain Healthcare, vol. 1, 2016, pp. 1– 10.
[39] Masiha, Mohammad Saeed, Amin Gohari, Mohammad Hossein Yassaee, and Mohammad Reza Aref. "Learning under Distribution Mismatch and Model Misspecification." arXiv preprint arXiv:2102.05695 (2021).
[40] J. Zhang, N. Xue, and X. Huang, “A secure system for pervasive social network-based healthcare,” IEEE Access, vol. 4, pp. 9239–9250, 2016.
[41] Kavousi, Alireza, J. Mohajeri and M. Salmasizadeh. “Improved Secure Efficient Delegated Private Set Intersection.” 2020 28th Iranian Conference on Electrical Engineering (ICEE) (2020): 1-6.
[42] A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” Journal of medical systems, vol. 42, no. 8, p. 140, 2018.
[43] Meisami, Sajad, Mohammad Beheshti-Atashgah, and Mohammad Reza Aref. "Using blockchain to achieve decentralized privacy in IoT healthcare." arXiv preprint arXiv:2109.14812 (2021).
[44] Aghabagherloo, Alireza, Javad Mohajeri, Mahmoud Salmasizadeh, and Mahmood Mohassel Feghhi. "An Efficient Anonymous Authentication Scheme Using Registration List in VANETs." In 2020 28th Iranian Conference on Electrical Engineering (ICEE), pp. 1-5. IEEE, 2020.

AUTHORS

Sajad Meisami is PhD candidate in Computer Science at Illinois Institute of Technology. Before that he received his M.Sc degree from Sharif University of Technology.

Mohammad Beheshti-Atashgah is graduate Researcher at ISSL lab at department of Electrical Engineering at Sharif University of Technology. He received his PhD degree in 2021. His research interests include Cryptography theory and Data Security and Privacy.

Mohammad Reza Aref is a professor in the department of Electrical Engineering at Sharif University of Technology. He received his PhD degree in Electrical Engineering from Stanford University. His research interests include Information Theory, Cryptography theory, Statistical signal processing and Communication theory. He is a member of the IEEE.