Blockchain Framework for Secured On-Demand Patient Health Records Sharing

Meryem Abouali, Kartikeya Sharma, Oluwaseyi Ajayi, Tarek Saadawi
Department of Electrical Engineering
City University of New York, City College, New York, USA, 10031
maboual000@citymail.cuny.edu, Kartikeyasharma04@gmail.com, Oajayi000@citymail.cuny.edu, Saadawi@ccny.cuny.edy

***Abstract*—The healthcare sector is constantly improving patient health record systems. However, these systems face a significant challenge when confronted with patient health record (PHR) data due to its sensitivity. In addition, patient's data is stored and spread generally across various healthcare facilities and among providers. This arrangement of distributed data becomes problematic whenever patients want to access their health records and then share them with their care provider, which yields a lack of interoperability among various healthcare systems. Moreover, most patient health record systems adopt a centralized management structure and deploy PHRs to the cloud, which raises privacy concerns when sharing patient information over a network. Therefore, it is vital to design a framework that considers patient privacy and data security when sharing sensitive information with healthcare facilities and providers. This paper proposes a blockchain framework for secured patient health records sharing that allows patients to have full access and control over their health records. With this novel approach, our framework applies the Ethereum blockchain smart contracts, the Inter-Planetary File System (IPFS) as an off-chain storage system, and the NuCypher protocol, which functions as key management and blockchain-based proxy re-encryption to create a secured on-demand patient health records sharing system effectively. Results show that the proposed framework is more secure than other schemes, and the PHRs will not be accessible to unauthorized providers or users. In addition, all encrypted data will only be accessible to and readable by verified entities set by the patient.**

***Index Terms*—Blockchain, Patient Health Records, Smart Contract, IPFS, NuCypher, Patient health records sharing, Healthcare System, Security, Privacy**

I. Introduction

The healthcare sector copes with massive patient information daily, which is sensitive, personal, and confidential. However, this data is often fragmented and spread across different healthcare facilities and providers, making it difficult for a patient to access it. As a result, neither the patient has control over his/her data nor can healthcare providers smoothly gain access to the patient's history when they need it for delivering quality care services. Furthermore, when medical treatments require patients' health records from multiple healthcare entities for diagnosis, medication, decision-making, and recommendations, they are often confronted by the lack of interoperability among these healthcare facilities.

Patient health records (PHR) are highly private, sensitive, and involve a significant security challenge in their management and sharing. Thus, the data must be confidential, secure, tamper-proof, and preserve integrity to avoid discrepancies. According to healthcare data breaches, the Health Insurance Probability and Accountability Act (HIPAA) statistics stated that the number of breaches into health records for 2019 was approximately three times more than in 2018 [1], which was estimated to be over 25 million data breaches regarding the health IT security. Fig.1 shows the number of breached health records over the year 2019.

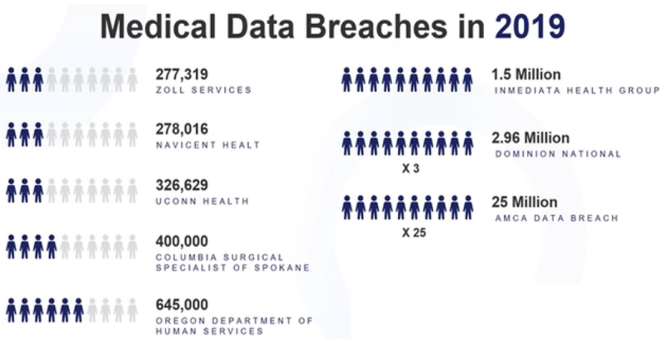

Fig. 1. The number of Health Record breaches of 2019.

Patient health records (PHR) systems have recently become fascinating for researchers regarding access management and data sharing. However, it is essential to ensure that PHRs are shared appropriately in a secure and tamper-proof environment which safeguards from any data breach given how it might be critical. The existing techniques are not appropriate for patient health records because of their centralized working principle of identity authentication and storage management sharing. To solve these issues, this paper provides secured patient health record sharing by leveraging the benefits of blockchain [2]. The main objective of the secure patient health records sharing (SPHRS) framework is to have a patient-centric system that enables efficient management and sharing of health records. The significant contributions of the paper are the use of Ethereum smart contracts, which allow us to provide data security and enhance data privacy through the verification and authentication of doctors, ensuring that unauthorized entities will not have access to sensitive health records. Distributed file system technology, IPFS, serves as a decentralized storage mechanism for PHRs, improving data integrity and data interoperability. Moreover, patient health records stored in IPFS are encrypted using NuCypher, a

layer two protocol built on Ethereum, which functions as a decentralized key management system and blockchain-based proxy re-encryption service.

The remainder of our paper is organized as follows: Section II discusses the problem statement and motivation. Section III presents related work and background. The proposed framework is illustrated in section IV. Section V explains the implementation. Performance evaluation is presented in section VI. Finally, section VII concludes the paper.

II. PROBLEM STATEMENT AND MOTIVATION

Patient healthcare records are scattered among different healthcare entities. The lack of interoperability among the healthcare facilities makes it difficult to access these healthcare records and share them with care providers to receive adequate service [3]. The problem resides in how these healthcare records are being managed, stored, and shared. The lack of cooperation in the healthcare sector forces data synchronization between different healthcare facilities to be a lengthy process.

Patient privacy is another problem as the storage system used to hold patient health records has inadequate security protocols [4]. With the inefficiency, the vulnerability of these systems, and the lack of a clear definition of health records ownership and access management, it is hard to identify and reduce the risk of future system failures appropriately. In addition, patients may face significant obstacles in personal healthcare data retrieval and sharing them among other care providers. Moreover, the existing distributed version control systems are primarily centralized. Hence, health records sharing can benefit from blockchain technology and decentralized storage system to improve security and scalability.

Motivated by the need of having a reliable, trusted, decentralized patient health records sharing, and with the increase in demand for health records, we need a responsible data-sharing model that can ensure that patient health records are successfully shared among authorized providers and address significant issues currently faced in healthcare industries. We propose a blockchain framework for secured on-demand patient health records sharing system (SPHRS) based on a patient-centric decentralized solution for managing and sharing patient health records. To improve the security of patient health record sharing, we devise a novel access control mechanism using smart contracts. Furthermore, the data sharing protocol is designed to manage user access to the patient health records system. Moreover, due to the public nature of IPFS and even though it is peer-to-peer system access controlled by Ethereum Blockchain, we use the NuCypher network for proxy re-encryption and policy control. Time-based policies help us control access to shared data and easily revoke or extend it based on the requirement. Our system can integrate with almost any existing system to ensure PHR's sharing privacy and security. The proposed framework makes the following contributions:

- Authentication and Verification: the framework introduces a provider authentication and transaction verification to detect any abnormal activities on accessing a patient's sensitive information and deny an unauthorized provider from accessing patient health records.
- Patients have complete control over their PHRs: as a patient-centric system, possessing all their data, they can share their records or revoke access within minutes.
- IPFS is used as off-chain storage: to store data in a tamper-proof distributed IPFS, which removes the need to trust the third party handling the centralized database. In addition, it provides fast PHRs retrieval capability.
- NuCypher is integrated with the Ethereum Blockchain: NuCypher allows the management of encryption and re-encryption keys while using a blockchain-based proxy re-encryption mechanism to store and share patient health records securely. In addition, it gives an access authorization design based on the creation of an access policy.
- Smart contracts for authentication and verification: Ethereum blockchain features the smart contract used to authenticate and verify the care provider and the healthcare entities, making it resilient to data accessed by an unauthorized provider.

III. RELATED WORK AND BACKGROUND

There have been several traditional solutions to deal with the problem of secure PHRs sharing. Blockchain is one solution that overcomes most limitations in the existing distributed environment by introducing a patient-centered health record. However, most existing frameworks that implement blockchain for health record sharing use the centralized storage system.

In [5], the authors introduced a protected framework for health records that supports identity management and user authentication format (PBBIMUA) scheme for e-health environment using personal biometrics and providing high efficiency with security. However, the main issue is scalability and cost. In [6], the authors introduced a user-centric health data sharing system that could enhance identity management and preserve data privacy for patients. However, they had not considered the problem of identity management and user authentication to protect data storage.

In [7], the authors proposed the MedShare model, which engages with the problem of medical data sharing among cloud service providers. Smart contracts were used to track data exchanges between untrusted parties. The performance of the proposed system was evaluated only through network latency measurements with theoretical analysis.

In [8] and [9], the authors have proposed a blockchain-based medical record sharing system that ensures patient privacy and integrity of medical data. The model provides immutability of a patient's record by using a distributed ledger. However, the framework has not considered the case when data is too large to support the blockchain.

In [10] and [11], the authors proposed a blockchain framework to address the data fragmentation issue in the healthcare system. The blockchain helps care providers store health records in a decentralized structure and make use of its immutability property. They have used smart contracts to transfer medical records. However, it uses cloud-based storage, leading to compromised sensitive medical information.

MedRec [12] is an Ethereum based record management system for EHRs. MedRec leverages blockchain to manage user authentication, confidentiality, and data sharing of the records. MedRec provides the patients with their medical records, immutable log, and easy access to their medical information across different providers. However, MedRec only integrates with the provider's current storage solution rather than presently patient-centric, patient-owned data.

All the above methods have not emphasized enough the issue of privacy and security, hence possessing a breach of integrity. Furthermore, cloud storage [13] is proposed for storing health records by relying on a third party which is a definite disadvantage. The same proposed schemes have not considered the case when the data size is too large to support the blockchain ledger. In this work, we have addressed these issues by adopting a decentralized system. Below we present a brief description of the main components represented in the proposed framework SPHRS system.

Blockchain [14]-[16] technology can create a tamper-proof, secure record of events in a distributed peer-to-peer network.It provides an immutable ledger of transactions for the data-sharing system [17], which means recorded transactions in the blockchain cannot be altered by any unauthorized user. Moreover, access control using blockchain can provide system transparency and mitigate data breaches. Any unauthorized access is detected and prevents malicious transactions. In addition to using smart contract [18], which provides strict access control policies to achieve authentication, user's verification, grant access to health records, detect and prevent potential threats to health records in a distributed manner.

The Interplanetary File System (IPFS) is introduced as a decentralized off-chain storage medium to meet the requirement of storing extensive data such as patient health records [19]. Each stored file is allocated a unique hash according to the file's content to identify it uniquely. So, if somebody uploads two files with the same hash value, IPFS pins them to the server and creates only one entry in the content addressed storage block. Due to this feature, IPFS has no access control, and files over IPFS can be directly accessed by their respective hash value. This makes it easier to integrate with blockchain.

NuCypher [20] is used to manage encryption and decryption keys. It is a decentralized blockchain-based key management system (KMS) encryption and access control service. It enables data sharing between users/nodes using proxy-re-encryption over the network. NuCypher uses decentralized network to delegate encryption/decryption rights. By delegating rights among multiple nodes, it ensures reliability, availability, and correctness through having no single point of failure. Upon using proxy-re-encryption, NuCypher makes sure that unencrypted symmetric keys and re-encryption keys are not accessible at once, keeping data protected. Hence, decentralized KMS helps conditionally grant and revoke access to sensitive data to an arbitrary number of recipients. NuCypher does that through policies that can be either time-based or condition-based. While we do not trust arbitrary miners in the system with encrypted data or re-encryption keys, we still trust them to create policies that control the duration of encryptions. Re-encryption is allowed only during a specific time interval, and the re-encryption key should be removed once the time is up.

IV. The Proposed Framework of SPHRS

In this section, we describe the details of our proposed scheme. It utilizes Ethereum blockchain [21] smart contracts to verify, authenticate and approve the access to the PHRs to ensure that unauthorized entities stay away from accessing patient health records. Then store the encrypted PHRS on IPFS to improve the integrity and interoperability. Our proposed SPHRS framework eliminates the need for a trusted centralized authority. It provides security and privacy to PHR sharing with high integrity and resiliency with the integration of NuCypher software to secure encryption re-encryption keys storing. Moreover, the patient does not have to interact directly with the care provider or the healthcare entities. Fig.2 The system model has the following entities:

- The patient is the data owner, and s/he holds total control over the data encrypted for her/him and determines with whom to share it.
- Healthcare entities are the encryptor, and they are PHRs source that encrypts data on behalf of the patient.
- The care provider is the data recipient that the patient intends to share data with.
- Ursula is the proxy in PRE. They are the nodes on the NuCypher network that stand ready to re-encrypt data in exchange for payment, and they enforce the access policy created by the patient.

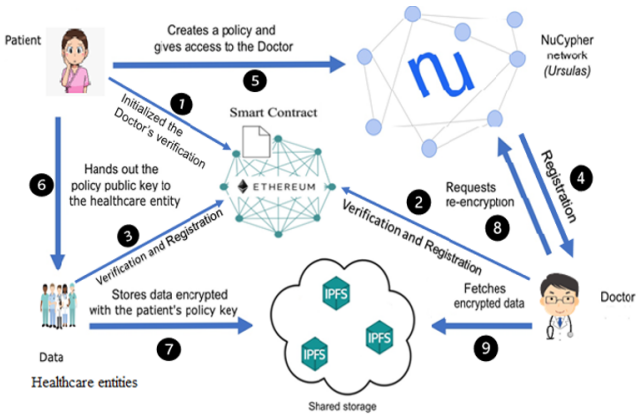

Fig. 2. Blockchain-based secured on-demand Patient Health Records Sharing.

V. Implementation

We consider an e-health scenario where patients can grant access to their health records stored by their healthcare entities and shared with their care providers. Our proposed framework SPHRS consists of four parts:

A. Authentication and Registration

Identity authentication is the biggest challenge in the cyber world. Therefore, we suggested a novel solution to solve this issue. The patient registers to the Ethereum Blockchain and is responsible for initiating a smart contract with the Provider's and healthcare entities' primary and general information to perform their identity authentication. When the provider and healthcare entities join the blockchain, they must enter the same information provided by the patient. If the information matches, they grant the access to create an account in the blockchain. Otherwise, their access is revoked. The patient initiates Algorithm 1 to verify the Provider and healthcare entities, while Algorithm 2 and Algorithm 3 are deployed by the provider and the healthcare entities consecutively to be authenticated. The proposed of these Algorithms is to prevent malicious entities from accessing the shared PHRs. Thus, identity authentication ensures the security of the model.

Algorithm 1: Doctor Verification

```
Procedure: Doctor verification
Inputs: patient address, doctor id

If Sender is Patient:
    If (Set Doctor):
        Add Doctor Id to Mapping
        Validate Transaction
        Return Success
    end if

    If (Query Doctor):
        Search Mapping for Doctor Id
        If (Mapping Exists):
            Validate Transaction
            Return Success
        else:
            Return Fail
        end if
    end if

    if (Change Patient):
        Set New Patient to Patient
        Validate Transaction
        Return Success
    end if
else:
    Return fail
    Drop transaction
end if
end procedure
```

Algorithm 2: Doctor Authentication

```
Procedure: Doctor Authentication
Inputs: general information, primary information

If Sender is Doctor:
    If (Set Doctor Information):
        Set Doctor Information
        Validate Transaction
        Return Success
    end if

    If (Set Primary Information):
        Set Primary Information
        Validate Transaction
        Return Success
    end if

else:
    Return fail
    Drop transaction
end if
end procedure
```

Algorithm 3: Healthcare Entity Authentication

```
Procedure: Healthcare Entity Authentication
Inputs: general information, primary information

If Sender is Healthcare Entity:
    If (Set Healthcare Entity Information):
        Set Healthcare Entity Information
        Validate Transaction
        Return Success
    end if

    If (Set Primary Information):
        Set Primary Information
        Validate Transaction
        Return Success
    end if

else:
    Return fail
    Drop transaction
end if
end procedure
```

B. Patient creates access policy for the provider

The patient and the provider create an account in the NuCypher network, which will generate the provider's public and private keys. NuCypher network features a proxy re-encryption mechanism, which enables sharing of sensitive data across public networks without revealing data keys to a third party. NuCypher generates a private key and policy public key from the label for the patient. For the patient to share his PHRs with the provider, he must create an access policy for the provider and use a proxy re-encryption mechanism to re-encrypt his private key and the provider's public key, then splits the re-encrypted key into "n" key fragments and send it to "n" different Ursulas and states how long data can be encrypted and who can decrypt it. When Ursulas receive the

access policy, they stand ready to re-encrypt data in exchange for payment in the form of rewards. Fig.3.

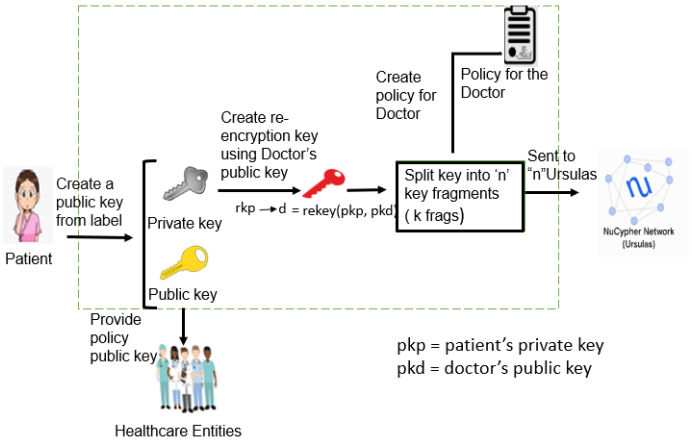

Fig. 3. Healthcare entities encrypt PHRs and upload them to IPFS.

C. Healthcare entities encrypt PHRs and upload them to IPFS

The patient hands out the public policy key to the healthcare entities to encrypt his PHRs. In return, healthcare entities generate a random symmetric key to encrypt the PHRs. Thus, it results in the ciphertext, while the capsule contains the symmetric key encryption with the patient's policy public key. Both the ciphertext and the capsule are stored in IPFS. Fig.4

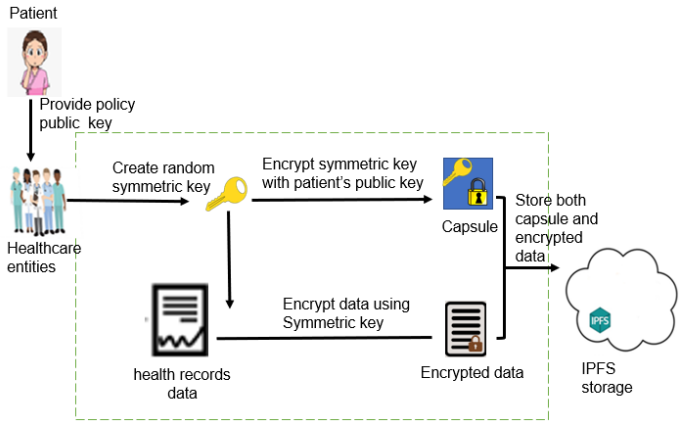

Fig. 4. Healthcare entities encrypt PHRs and upload them to IPFS.

D. Provider retrieves the patient's health records

The provider obtains the capsule and the ciphertext that contains the encrypted patient's health records from IPFS storage. For the provider to have access to PHRs, he must communicate with several Ursulas to request re-encryption of the capsule because the patient previously distributed Kfrags for his policy among them. Then the capsule is encrypted with the provider's public key and decrypted with the provider's private key to obtain the symmetric key. Now the provide decrypts the PHRs using the symmetric key. Fig.5

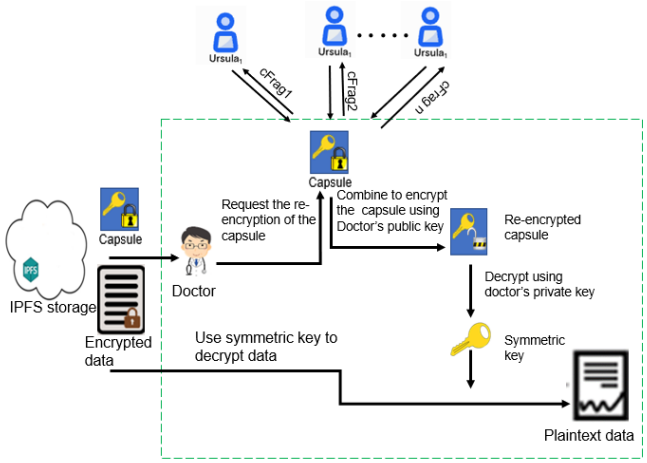

Fig. 5. Provider decrypts the symmetric key then decrypts PHRs.

VI. Discussion and Analysis of the Aspects of the Proposed Framework

In this section, we discuss and analyze the framework's security and privacy properties and other parameters.

A. Integrity

In our proposed framework, integrity guarantees that PHRs are shared between authorized users without changing information. Any unauthorized user cannot alter the data stored in this system. Therefore, the PHRs are available to only authorized users who are granted the patient's right to access them. In addition, the encrypted data is stored on IPFS to ensure security.

B. Confidentiality

Our framework preserves the confidentiality of the PHR data, which is encrypted using a proxy re-encryption mechanism, and only the authorized users have access to the records for a particular time. Any untrusted third party denies access. The patient has complete control over his PHRs and can revoke access at any point.

C. Privacy

In the PHRs sharing, our access control scheme guarantees data privacy and patient control over his health records. Malicious access is blocked by the user's identity authentication protocol and smart contract authorization to prevent potential threats from accessing our IPFS storage. The patient re-encrypts the keys using proxy re-encryption and creates the access policy. Therefore, only the provider whose attributes satisfy the access policy can obtain the PHRs.

D. Security

In our scheme, multiple levels of protection exist to ensure security. The utilization of proxy re-encryption mechanism ensures confidentiality as only the patient and provider access PHRs. The PRE does not expose the private keys of the users. Furthermore, the access policy combined with blockchain

solutions embraces a high level of identity authentication by implementing the smart contracts functionality. In addition, IPFS guarantees the security of the stored encrypted data.

E. Scalability

Our proposed framework provides an off-chain storage mechanism IPFS to solve the issue of limited storage capacity of the blockchain and the massive volume of the PHRs size. It demonstrates and proves that the current PHRs sharing system is capable of processing large PHRs. In addition, the PHRs can be encrypted just once by the healthcare entities, and the patient may create multiple policies and grant access to multiple care providers to access them.

F. Avoid a single point of failure.

Unlike the traditional cloud storage solutions, our proposed scheme employs the decentralized Ethereum blockchain, storage system IPFS, and NuCypher network, which all are distributed technologies. As a result, even if some nodes fail or get compromised, the entire scheme's availability will not be affected. This effectively solves the single point of failure.

VII. Conclusion

This paper proposes a novel and secure PHRs system based on the Ethereum blockchain and IPFS. Proxy re-encryption is adopted to bring a distributed access control and key management to the system. We identify critical security, privacy, data fragmentation, and vulnerability in the current client/server and cloud-based approaches, and we propose efficient solutions to address these issues through an actual prototype implementation. In this work, we design a reliable access control mechanism based on a smart contract and policy. Furthermore, its flexibility targets a specific use case and can be generalized for a wide range of other problems and adapted to other systems. In our future work, we plan to evaluate the performance measures of our proposed framework and investigate how it protects against the insider threat and extend this implementation work to the real-time application for the healthcare system by adding a large number of users.

Acknowledgment

This work is supported in part by NSF JUN02(Japan-US Network Opportunity 2) (Award No. 1818884) and NSF IRNC (Award No. 2029295)

References

[1] Jessica Davis (2019) "The 10 Biggest Healthcare Data Breaches of 2019, So Far" by Health IT Security. https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

[2] Shrestha, A.K.; Vassileva, J. Blockchain-Based Research Data Sharing Framework for Incentivizing

[3] Kirsh, D., W. K, and W. K., "How outdated medical record systems and devices could risk lives," URL https://www.medicaldesignandoutsourcing.com/outdated-medical-record-systems-devices-risk-lives/.

[4] URL https://en.wikipedia.org/wiki/Electronic_health_record."Electronic health record."

[5] Xinyin Xiang, Mingyu Wang, Weiguo (Patrick) Fan, "A Permissioned Blockchain-based Identity Management and User Authentication Scheme for E-health Systems" IEEE Access,2016.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commu. (PIMRC), Oct. 2017, pp. 1–5.

[7] Q. I. 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

[8]] Alexaki, S., Alexandris, G., Katos, V., Petroulakis, E. N. (2018, September). Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. In 2018 IEEE 23rd International Workshop on Computer-Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

[9] De Oliveira, M. T., Reis, L. H., Carrano, R. C., Seixas, F. L., Saade, D. C., Albuquerque, C. V., ... Maos, D. M. (2019, May). Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE

[10] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," 2018 IEEE 20th International Conference on e-Health Networking Applications and Services (Healthcom), pp. 1-7, Sep. 2018.

[11] Thomas K. Dasaklis, Fran Casino," Blockchain Meets Smart Health: Towards Next Generation Healthcare Services," 978-1-5386-8161-9/18©2018 European Union

[12] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD), 25-30.

[13] Dubovitskaya, A., Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain",URL https:// www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/the Data Owners. In International Conference on Blockchain; Springer: Cham, Switzerland, 2018; pp. 259–266.

[14] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," J. Amer. Med. Inf. Assoc., vol. 24, no. 6, pp. 1211–1220, 2017.

[15] Mettler, M. Blockchain Technology in Healthcare: The Revolution Starts Here. In Proceedings of the IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–3.

[16] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," Comput. Struct. Biotechnol J., vol. 16, pp. 224–230, 2018.

[17] M. Hölbl, M. Kompara, A. Kamišalic, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," Symmetry, vol. 10, no. 10, p. 470, 2018.

[18] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38437–38450, Jun. 2018.

[19] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).

[20] A. Ghazvini and Z. Shukur, "Security challenges and success factors of electronic healthcare system," Procedia Technol., vol. 11, pp. 212–219, 2013.

[21] O. Ajayi, M. Abouali and T. Saadawi, "Secured Inter-Healthcare Patient Health Records Exchange Architecture," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 456-461.