Secure Architecture for Inter-Healthcare Electronic Health Records Exchange

Conference Paper · August 2020

DOI: 10.1109/IEMTRONICS51293.2020.9216336

3 authors, including:

Oluwaseyi Ajayi
City College of New York
3 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Tarek Saadawi
City College of New York
250 PUBLICATIONS **3,832** CITATIONS
SEE PROFILE

Secure Architecture for Inter-Healthcare Electronic Health Records Exchange

Oluwaseyi Ajayi
Department of Electrical Engineering, City College of New York,
New York, USA
Oluwaseyi.j.ajayi@gmail.com

Meryem Abouali
Department of Electrical Engineering, City College of New York,
New York, USA
Maboual000@citymail.cuny.edu

Tarek Saadawi
Department of Electrical Engineering, City College of New York,
New York, USA
sadaawi@ccny.cuny.edu

Abstract—**The increase in cyberattacks against the healthcare system, notably Electronic Health Records (EHRs) breaches, has cost the healthcare providers more in recent years. This situation is predicted to increase in the coming years as the healthcare systems are proposing a consortium EHRs repository. Due to this reason, it is crucial to deploy solutions that can ensure the security of shared health records. More specifically, maintaining the integrity and consistency of shared EHRs becomes pertinent. In this on-going research, we propose a blockchain-based solution that facilitates a scalable and secured inter-healthcare EHRs exchange. These healthcare systems maintain their records on individual private blockchain networks, and the blockchains interact to exchange patient health history based on request. The proposed solution verifies the integrity and consistency of requests and replies from other healthcare systems. It presents them in a standard format that can be easily understood by different healthcare nodes. The verification steps guard against malicious activities on both stored and in transit EHRs from insider and outsider threat actors. We evaluate the security analysis against frequently encounter outsider and insider threats within a healthcare system. The preliminary result shows that the architecture can detect and prevent threat actors from uploading compromising EHRs into the network and prevents unauthorized retrieval of patient's information.**

Keywords— Blockchain, Electronic Health Records, Compromised EHR, Healthcare System, Security, Data Integrity, Consistency.

I. INTRODUCTION

The tremendous increase in the healthcare record breaches has made healthcare interoperability more challenging to achieve. In 2019, around 572 recorded attacks in the U.S. healthcare industries resulted in over 41 million patient record breaches, and it is estimated to jump up by 60% in 2020 [1]. The effects of these attacks are estimated to cost the industry about $1.4 billion a year. Although ransomware attack accounts for about 58% of the total breach, staff members inside the healthcare organization were responsible for about 9.2% of the data breach in 2019 [2]. Due to the prevalence of attacks on patient records, there is an urgent need to deploy a more secure method to protect Electronic Health Records (EHRs) shared among different healthcare systems, especially now that healthcare systems are proposing more robust interoperability. For the proposed interoperability to work, the integrity and consistency of the stored or shared EHRs must be guaranteed. Thus, it is crucial to have a solution that detects and prevents malicious activities in EHRs. Over the years, healthcare systems have utilized a firewall to protect stored EHRs [3-7]. [3] iimplements the firewall to serve as an anomaly-based intrusion detection system (IDS). In the implementation, the firewall is either configured as a packet filtering firewall or status inspection firewall. The authors in [8] put forward encryption to ensure the security of EHRs during the exchange process. This approach was designed by Health Insurance Portability and Accountability Act (HIPAA) to secure EHRs when viewed by patients or when creating, receiving, maintaining, or transmitting Patient Health Information (PHI) by mobile devices. Despite the success of the approaches, the malicious intruders still find ways to subvert these protection systems and gain unauthorized access to EHRs.

Healthcare providers believe that their data is secured as far as it is encrypted. Although encryption guarantees the confidentiality of such data, consistency, and integrity are not guaranteed. [9] proposed a message authentication code algorithm (MAC) for detecting any changes in stored data. Although this approach detects changes in the stored data, it is not practical for extensive data because downloading and calculating MAC of large files is overwhelming and time-consuming. Another method described in [9] secures cloud data integrity by computing the hash values of every data in the cloud. This solution is lighter than the first approach in [9]. However, it requires more computation power, especially for massive data; hence, it is not practical. The authors in [10] employ the third party to coordinate activities of the database. The problem with this approach is that the data is vulnerable to man-in-the-middle or single-point-of-failure attack.

Further research has put forward the application of blockchain technology in handling, protecting, and interacting IoT devices with personal EHRs [10-17]. The approaches described in these researches prove effective in handling and protecting stored personal EHRs. However, the proposed solutions cannot be applied to the EHRs exchanged between two or more healthcare systems as they are primarily focusing on securing and protecting personal EHRs. In this research, we propose a solution that leverages the tamper-proof ability, data immutability, and distributive ledger ability of blockchain to share EHRs among different healthcare systems securely.

The new dimension in the healthcare industry is the interoperability of different healthcare systems. The interoperability is important because a patient's diagnosis

978-1-7281-9615-2/20/$31.00 ©2020 IEEE

and treatment journey can take them from a physician's office to an imaging center or the operating room of a hospital. Each stop generates a record, such as doctor's notes, test results, medical device data, discharge summaries, or information essential to the social determinants of health, which become part of a patient's electronic health record in each setting. For the best outcome, this health information should be accessible and securely exchanged among all sources that accompany the patient's treatment every step of the way. This interoperability will strengthen care coordination and improve safety, quality, efficiency, and encouragement of robust health registries. However, most of the available solutions in hospitals use fax messages for EHR exchange between healthcare systems, and cloud database for storing EHRs. The significant problems facing the currently available solution are (i). The medium of exchange can be hacked, thereby compromising the integrity and consistency of the shared data. (ii) The database housing the EHRs can be hacked, and data can be manipulated or deleted. (iii) Lack of universal format for EHRs exchange makes it difficult to detect and prevent malicious activities.

We propose a solution that ensures the integrity and consistency of shared health data, presents a standard format for exchanging EHRs, and detects any malicious activities on stored and shared EHRs. Hence, the contributions of our work can be summarized as follows:

- We propose a blockchain-based architecture that facilitates a scalable and secured inter-healthcare EHRs exchange among different healthcare systems.
- The proposed architecture detects and prevents malicious activities on both stored and shared EHRs from either outsider or insider threats.
- The architecture verifies the integrity and consistency of EHR requests and replies, then presents them in a standard format easily understood by the different healthcare systems.
- The architecture permanently stores the verified EHRs in a distributive ledger and shares with other health care systems securely when requested.
- The proposed architecture is robust to a new healthcare system joining the network in real-time.

The remainder of this paper is organized as follows: related works on blockchain application in healthcare are discussed in Section II. Section III describes the proposed architecture, while the preliminary result is presented in section IV. Section V presents the conclusions of this paper and possible future works.

II. RELATED WORKS

A. Blockchain application in healthcare

First introduced as the technology behind bitcoin in 2008 [18], blockchain was implemented to solve the double-spending problem in a cryptocurrency called bitcoin. Since its inception, diverse areas have seen the application of blockchain technology. e.g., health system [10-17], data integrity [19], [29-30], intrusion detection system [20-22], and so on. Blockchain is an append-only public ledger that records all transactions that have occurred in the network. Every participant in a blockchain network is called nodes. The data in a blockchain is known as a transaction, and it is divided into blocks. Each block is dependent on the previous one (parent block). So, every block has a pointer to its parent block. Each transaction in the public ledger is verified by the consensus of most of the system's participants. Once the transaction is verified, it is impossible to mutate/erase the records [18]. Blockchain is broadly divided into two: public and private blockchain [23]. A public blockchain is a permissionless blockchain in which all nodes do verification and validation of transactions. e.g., Bitcoin, Ethereum. While private blockchains are permissioned blockchains where only nodes given permission can join and participate in the network. e.g., Hyperledger.

Blockchain application in EHRs is still in its inception. However, the potential it offers, the deficiencies and gaps it fills and ensuring the security and confidentiality of health data make it the forefront to be adopted in the healthcare industry nowadays. Blockchain technology has been applied to different kinds of researches to secure personal data. The authors in [24] propose a platform that enables a secure and private health record system by separating sensitive and non-sensitive data. The platform serves to share a patient's healthcare data with researchers without revealing the patient's privacy. The model successfully uses proxy re-encryption techniques to share a patient's sensitive data without revealing the patient's private key and adopting an asymmetric cryptography technique to encrypt these data while storing it on the cloud. Another similar work [25] proposes i-Blockchain, which uses a permissioned blockchain to preserve the privacy of the Patient's Health Data (PHD) and improve the individual's experience in data exchange. It allows only qualified individuals and Healthcare Service Providers (HSP) to join the network to prevent malicious attacks. It uses cold storage functions as off-blockchain storage and hot storage functions as the store where users temporarily put requested data in addition to a private key and a public key for secure data exchange.

Furthermore, [26] proposes the conceptual design for sharing personal continuous dynamic health data using blockchain technology. The approach is supplemented by cloud storage. The authors proposed using hash pointers to the storage location to solve the problem of sharing large-sized continuous-dynamic data while integrating blockchain and cloud storage. Extensive size data can be stored in an encrypted format on the cloud, and only the transactional data and metadata can be saved and shared on the blockchain. The authors in [27] propose a decentralized record management system (MedRec) to manage authentication, confidentiality, accountability, and data sharing of EHRs using blockchain technology. It is a modular design that integrates with patient's local data storage and encourages medical stakeholders to participate as miners. The result shows that the system enables the emergence of big data to empower researchers while engaging the patient and providers in the choice of release metadata. [28] proposes a new approach which joins blockchain and cloud computing network. In their work, they employ Amazon Web Services and Ethereum blockchain to facilitate the sematic level interoperability of EHRs systems without standardized data forms and formatting. The model proposes an interoperability data sharing framework that includes security through multilayer encryption, optical data

storage through Amazon Web Service, and transfer using the Ethereum blockchain.

Despite the researches on blockchain application in healthcare, most of the available solutions focus on securing and sharing personal EHRs, failing to address the security of health records shared between two or more healthcare systems. The lack of secure exchange of EHRs is the motivation for this work. The novelty in the proposed solution is to facilitate a scalable and secured inter-healthcare EHRs exchange while detecting and preventing malicious activities on the data. This novelty distinguishes our work from previous works.

III. THE PROPOSED ARCHITECTURE

The proposed architecture, which focuses on securing inter-healthcare EHRs exchange, is implemented on the Hyperledger Fabric blockchain platform. The Hyperledger fabric features a chaincode which houses the smart contract. The chaincode is deployed to the fabric, and each peer interacts with the code. The smart contract keeps the agreement among consortium members, and all participants run it. Fig. 1 shows a pictorial representation of the proposed architecture.

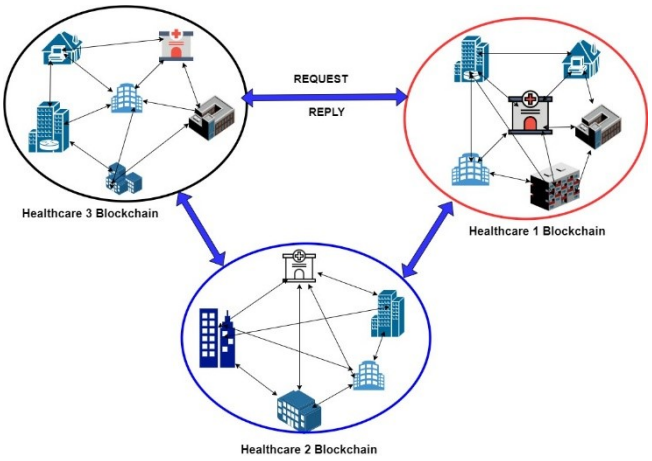

Fig. 2. The Proposed Architecture

The architecture comprises of different healthcare systems running private blockchain networks. Each blockchain network is independent of each other and features a unique smart contract that is written according to the healthcare system and HIPAA's policies. In each healthcare system, computers used in collecting patient records from peers in a private blockchain network. The peers in each network prepare, submit, verify, and keep a copy of the ledger of all transactions (i.e., patient's EHRs). The peers also run the consensus algorithm, thus validate transactions/blocks. The peers similarly validate the transactions, as described in our previous works [29,30]. However, unlike the previous works, which uses public-private blockchain networks, we set up a fully private blockchain network for each healthcare system.

In this current work, we focus on investigating a secured exchange of patients' records among different healthcare systems. In this implementation, the healthcare systems keep and maintain patient health information on individual private blockchain networks. We describe the process of interaction and exchange of the patients' EHRs among them. We deploy a smart contract on each private blockchain platform via chaincode. The smart contract handles the verifications of all transactions. In this context, we define a transaction as any of the following:

1. A patient's health information about to be stored into the blockchain network
2. A request for patients' medical history from another healthcare system.
3. A reply that carries the requested patient's information

This paper describes how the architecture achieves the verification and validation of requests and replies to mitigate malicious activities. (i.e., we describe how a request for a patient's health history undergoes different security verification and validation before being sent to the closed primary healthcare system.)

The proposed architecture is divided into three main steps, as shown below.

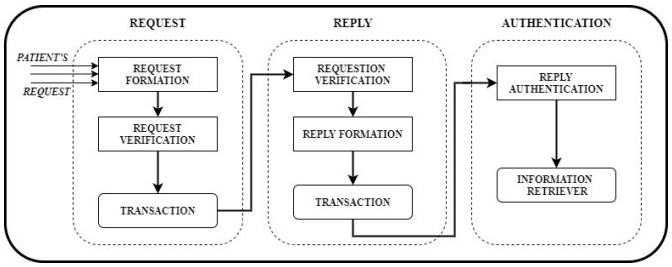

Fig. 3. Building blocks of the proposed architecture

A. Request

The request stage is subdivided into three categories: request formation, request verification, and transaction formation. The request is formed to obtain a patient's medical history from another healthcare center or medical test results from a laboratory. For example, a person who lives in New York, USA, travels to London, UK. If the person had to visit the hospital for treatment, the medical history should be retrieved from the New York hospital for better medical treatment. The medical records can be retrieved by preparing a request with information that is unique to the patient. During the process, a requester (doctor or nurse in the visiting hospital) supplies the required information to a developed script running on the peers. This script captures the patients' information such as name, date of birth, Social Security Number (SSN), name of the former healthcare system, and requester's unique code.

The script verifies the information and the identity of the requester. The request is developed into an agreed-upon format, digitally signed by the peer, and submitted as a transaction to the hospital's blockchain network. Apart from the submitted transaction, the peer (node) submits its information, which includes the requester's unique code, the MAC address, and the peer's transaction address. The smart contract run on the blockchain verifies the transaction's format, the requester code, and the peer's identities. The purpose of the verification is to detect and prevent all unauthorized activities on the transaction. Algorithm 1 below describes the snippet of the smart contract that

handles the verification process. Since the healthcare blockchains communicate via smart contracts, each smart contract running on the blockchain networks contains the processes described in algorithm 1.

The smart contract verifies the transaction by comparing the format with the stored transaction format. It checks the number of requests from the same peer within a minute and compares it to a maximum value. We set the maximum value of request from a peer to 1. It also checks if the destination address is found in the blockchain lookup table. It confirms the privilege of the peer to submit transactions by verifying its digital signature with its public key. It further checks for the peer's information in the information lookup table and verifies the health worker's code. Apart from the above, the smart contract controls each peer's right to assess patients' records. For a request to be successful, it must agree with a standard format, and the number of requests per minute must not exceed a maximum value. Also, the requester must be authorized, destination healthcare blockchain must be available and correct, peer's information must be correct, and the peer's public key must verify its private key. If any of these verification steps fail, the transaction is dropped. A successful request is validated and attached to the blockchain. The validation process has been described in our previous works [29,30].

Algorithm 1: Request Verification

Procedure: Verification **(Request)**
Inputs: formatted request/reply, Peer Information

```
If (Request agrees with Standard Format) and
    (No. of Requests/min <= Max) and
    (Requester code in authorized code sets) and
    (Destination in lookup table) and (Peer Information is verified)
     and (public key verifies private key):

        Validate Transaction
          Return Success
else:
          Return fail
          Drop transaction
end if
end procedure
```

B. *Reply*

After a successful validation process, the smart contract routes the request to the designated healthcare network based on the lookup table. The smart contract verifies the format of the received request and the requesting network. Algorithm 2 below describes the pieces of the smart contract that handles the verification of an incoming request. The source information, format of request, and digital signature of the source healthcare are verified. The supplied information about the patient is confirmed. For an incoming request to be successful, the request's format must agree with the standard, source information must pass verification step, requested EHRs must be available in the healthcare network, and the source public key must verify its private key. If any verification steps fail, the request is dropped, and a failed request is issued to the source network. A successful request is validated and attached to the blockchain. Based on the required information, the peers compete to prepare a reply by retrieving the patient's EHRs from the blockchain network. The peer that first prepares the information submits it as a transaction to the blockchain for verification. The transaction is verified as explained in algorithm1. A successfully verified reply is validated and routed back to the source network.

Algorithm 2: Reply Formation

Procedure: Reply formation by destination network
Inputs: request, Source Information (S.I).

```
If (Request agrees with Format) and
    (S.I in lookup table) and
    (Patient's EHRs in Destination Healthcare) and
    and (public key verifies private key):

          Return Success
          Validate the request and form reply
else:
          Return fail
          Drop request
end if
end procedure
```

C. *Authentication*

The source network verifies the incoming reply. The smart contract verifies the format of the information, the address of the reply's network, and the digital signature of the reply's network in a way showed in algorithm 3. When the verification process is successful, the transaction (reply) is validated and attached to the blockchain. The blockchain is updated, and the newly added block reflects on the ledger of every peer in the network. Every blockchain peer possesses a copy of this ledger. All blockchain peers receive the notification of the newly added block but do not have access to the block's content. The requesting node retrieves the information in the block, and a developed script converts it to a format that can easily be understood by the requester (healthcare work).

Algorithm 3: Reply Verification

Procedure: Verification **(Reply)**
Inputs: formatted reply, Source Information

```
If (Reply agrees with Standard Format) and
    (Request destination matches reply source) and
    (source Information in respective sets) and
    (source digital signature is verified):

          Validate reply
          Return Success
else:
          Return fail
          Drop reply
end if
end procedure
```

IV. RESULTS

We carry out the implementation of the proposed architecture in the laboratory. We set up two different Hyperledger fabric blockchain networks (I and II) with each network comprising of three peers. For each blockchain network, we installed Hyperledger Fabric *v2*, use *Golang v1.14* implementation for smart contract and *docker v19.0.3 and docker-compose v1.26.2, nodejs v12.18.1, npm v6.4.1*and *python v3.6*. All the blockchain peers run Linux Ubuntu *v18.04* operating system. The smart contract is written as described above and deployed into the blockchain channels. The MAC and transaction addresses of all peers are written as lists in the smart contract. A list that stores the requester code is also included in the smart contract. The format of requests and replies and the requester's unique codes are coded in the smart contract. Apart from this, the smart contract also contains a lookup table that stores information about the blockchain II. We write a similar smart contract (with blockchain I information) for blockchain II. A transaction (request for patients' medical history) was prepared as explained in section III and submitted as a transaction to the blockchain network I. In the security analysis, we anticipated and tested ways an insider or outsider malicious intruder could attempt to compromise a request within a healthcare system. We performed the attack and presented the result obtained from our architecture. In the outsider attack, we implement how the architecture detects and prevents unauthorized peers from submitting a transaction to the blockchain network. While for the insider attack, we showed how the architecture detects a compromised peer and prevents it from inserting its transaction.

A. SECURITY ANALYSIS

1) Outsider Threat Detection

We present the security result of the architecture against malicious transaction injection into the blockchain. Here, we added a peer (malicious node) that was not part of the blockchain to network I. We assume that an attacker may find its way into joining the blockchain. The malicious node prepares a request transaction and submits it to the blockchain network for verification. Although the transaction agrees with the standard, we observed that a failed transaction notification was sent to the owner. The transaction failed because the sender is not authorized to submit a transaction; hence, it fails the verification step. We manually created the transaction address and used it to check if the transaction is validated and stored in the ledger. The result shows that no transaction is retrieved; hence the transaction is not uploaded to the blockchain network.

2) Insider Threat Detection

Here, we tested the security of the architecture against two typical ways a malicious insider can have unauthorized assess to patient's health records.

a) Multiple Requests: We performed an attack where a malicious insider compromises a peer and begins to send a large amount of what appears to be a legitimate standard formatted request to mount a DoS attack on the blockchain network. The peer prepares a request transaction and submits it to the blockchain. The peer persistently submits the same transactions to mount a DoS attack on the blockchain network. Although other authorized nodes are working to validate the transaction, we observed that the transactions are not validated. The frequency of receiving the same or similar transaction from the same peer exceeds the threshold set in the smart contract. As a result of that, the transactions failed the verification step. We persistently submit the same request from the same authorized node, and we observed that the peers stop mining after the sender was flagged to be compromised. The smart contract automatically drops all subsequent transactions from the same peer.

b) *Unauthorized retrieval of patient's record*: We implement a case where a malicious insider attempts to retrieve patient information. It is assumed that an attacker is unlikely to hold an authorized peer in a compromised state for too long due to frequent security checks. Based on this assumption, an attacker makes all efforts to assess the patient's medical record within the shortest time possible. The result showed that no information was returned because the peer not authorized to retrieve the information. In the smart contract, information retrieval privilege is set for each peer (i.e., the node can only retrieve information that it prepares the request). The architecture drops the query because the node has no retrieval privilege for that patient's EHRs, which makes it suspicious to have been compromised.

V. CONCLUSION

In this on-going research work, we propose a blockchain-based architecture that facilitates and secures inter-healthcare EHRs exchange. In the implementation, each healthcare system maintains patient health information on private blockchain networks. The work focuses on improving the security of both stored and in transit EHRs to strengthen the interoperability between healthcare systems. We present the preliminary result of the security analysis on the detection and prevention of malicious transactions within a healthcare system. The result shows that our architecture has a prospect of detecting and preventing malicious activities from either insider or outsider threats.
As part of the continuation of the work, we wish to expand our work to accommodate the following:

1. Test for more malicious activities within a healthcare system.
2. Evaluate how to detect malicious replies or requests coming for another healthcare system.
3. Evaluate the scalability and its Response time.

REFERENCES

1 J. Clement (2020), Number of U.S. data breaches 2013-2019,

2 Heather Landi (2020), number of patients records breached nearly triples in 2019.

3 V. Liu, MA. Musen, T. Chou, "Data breaches of protected health information in the United States. Jour. of Amer. Med. Assoc. vol 313, num 14, (2015) pp. 1471–1473.

4 Jannetti MC. Safeguarding patient information in electronic health records. AORN vol. 100, num 3, (2014) pp. C7–C8.

5 Hunter, E.S., Electronic health Records in an Occupational Health Setting--Part I. A global overview. *Workplace health & safety*. Vol 61, num 2, (2013) pp.57–60.

6 Lemke J. Storage and security of personal health information. OOHNA J. vol 32, num 1, (2013) pp 25–26.

7 Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. JAMA. Vol. 313, num 14, (2015) pp 1471–1473.

8 Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. JAMA. Vol. 310, num 11, (2013) Pp.1121–1122.

9 Sultan Aldossary, William Allen. Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016 pp.485-498

10 C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, (2013) pp. 362–375, Feb 2013

11 X. Yang, T. Li, R. Liu, and M. Wang, "Blockchain-Based Secure and Searchable EHR Sharing Scheme," 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 2019, pp. 822-8223,

12 X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6.

13 S. Amofa et al., "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6.

14 K. Ito, K. Tago, and Q. Jin, "i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data," 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, 2018, pp. 829-833.

15 G. Yang and C. Li, "A Design of Blockchain-Based Architecture for the Security of Electronic Health Record (EHR) Systems," 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia, 2018, pp. 261-265.

16 P. Zhang, M. A. Walker, J. White, D. C. Schmidt and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom),* Dalian, 2017, pp. 1-4, doi: 10.1109/HealthCom.2017.8210842

17 X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361.

18 S. Nakamoto (2008) Bitcoin: a peer-to-peer electronic cash system.

19 Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., Yalansky, L.: Ensuring data integrity using Blockchain technology. In: Proceeding of the 20th Conference of fruct Association ISSN 2305-7254 IEEE (2017)

20 M Signorini and M Pontecorvi, W Kanoun, and R Di Pietro, "BAD: a Blockchain Anomaly Detection solution" arXiv:1807.03833v2, [cs. C.R.] 12 Jul 2018

21 T. Golomb, Y. Mirsky, and Y. Elovici " CIoTA: Collaborative IoT Anomaly Detection via Blockchain" arXiv:1803.03807v2, [cs.CY] 09 Apr 2018

22 Gu, J, B Sun, X Du, J Wang, Y Zhuang and Z Wang (2018). Consortium blockchain-based malware detection in mobile devices. IEEE Access, 6, 12118–12128

23 Abdullah, N., Hakansson, A., & Moradian, E. (2017). Blockchain-based approach to enhance big data authentication in distributed environment. In Ubiquitous and future networks (icufn), 2017 ninth international conference on (pp. 887–892).

24 V. Mahore, P. Aggarwal, N. Andola, Raghav and S. Venkatesan, "Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain," 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.9066204.

25 K. Ito, K. Tago and Q. Jin, "i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data," *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, 2018, pp. 829-833, doi: 10.1109/ITME.2018.00186.

26 X. Zheng, R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere, "Blockchain-based Personal Health Data Sharing System Using Cloud Storage," *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, 2018, pp. 1-6, doi: 10.1109/HealthCom.2018.8531125.

27 A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

28 G. Carter, H. Shahriar and S. Sneha, "Blockchain-Based Interoperable Electronic Health Record Sharing Framework," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 452-457, doi: 10.1109/COMPSAC.2019.10248.

29 O. Ajayi, M. Cherian and T. Saadawi, "Secured Cyber-Attack Signatures Distribution using Blockchain Technology," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 482-488, doi: 10.1109/CSE/EUC.2019.00095.

30 O. Ajayi, O. Igbe and T. Saadawi, "Consortium Blockchain-Based Architecture for Cyber-attack Signatures and Features Distribution," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York City, NY, USA, 2019, pp. 0541-0549, doi: 10.1109/UEMCON47517.2019.8993036.