Blockchain Architecture for Secured Inter-Healthcare Electronic Health Records Exchange

Oluwaseyi Ajayi[1], Meryem Abouali[1], Tarel Saadawi[1]
[1]City University of New York, City College, New York, NY 10031 USA
Oajayi000@citymail.cuny.edu, maboual000@citymail.cuny.edu, saadawi@ccny.cuny.edu

Abstract. 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 separate blockchain networks and are independent of each other. The proposed architecture can detect and prevent malicious activities on both stored and shared EHRs from either outsider or insider threats. It can also verify the integrity and consistency of EHR requests and replies from other healthcare systems and presents them in a standard format that can be easily understood by different healthcare nodes. In the preliminary result, we evaluate the security analysis against frequently encounter outsider and insider threats within a healthcare system. The result shows that the architecture detects and prevents outsider threats from uploading compromising EHRs into the blockchain and also prevents unauthorized retrieval of patient's information.

1 Introduction

Recently, the rapid increase in the cyberattack launched at Healthcare systems has become a significant concern. In 2019, over 572 recorded data breaches in the U.S. health care industries have breached over 41 million patient records, and it is estimated to jump up by 60% in 2020 [1]. The effects of these cyberattacks 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 protect and secure stored data and exchanged data among different healthcare systems, especially now that healthcare systems are proposing more robust interoperability. One of the significant techniques to protect Electronic Healthcare Records is the use of firewall [3-7]. [3] implements 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 as a way of ensuring 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 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 interaction of IoT devices with personal EHRs [10-17]. The approaches described in those research 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 focused on securing and protecting personal EHRs; hence, the motivation for this work. In this on-going research, we propose a solution that leverages the tamper-proof ability, data immutability, and distributive ledger ability of blockchain technology to exchange secured EHRs among different healthcare systems without any security concerns. The new dimension in the healthcare industry is the interoperability of different healthcare systems. The interoperability is important because a patient's diagnosis and treatment journey can take them from a physician's office to an imaging center, to the operating room of a hospital. Each stop generates a record, such as doctors' notes, test results, medical device data, discharge summaries, or information pertinent 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 needs to be accessible and securely exchanged among all sources that accompany patient's treatment every step of the way. This outcome will not only strengthen care coordination but also improve safety, quality, efficiency, and encouragement of robust health registries. Most of the available solutions use a fax message 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, both insider and outsider attackers.

We are proposing a solution that ensures the privacy and consistency of shared data, presents a standard format for exchanging EHRs, and detects any malicious activities

on stored and shared EHRs by either insider or outsider threats. 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 Electronic Healthcare Records (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 from other healthcare systems and presents them in a standard format easily understood by the different healthcare system
- The architecture permanently stores the verified EHRs distributively, and shares with other health care systems securely when requested.
- The proposed architecture is robust to a new healthcare system joining and leaving the network in real-time.

The remainder of this paper is organized as follows: Section II discusses the background and related works on application blockchain technology in healthcare. Section III describes the proposed architecture. Section IV presents the results, while section V presents the conclusions of this paper and possible future works.

2 Background and Related Works

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 security [19], as an intrusion detection system [20-22]. 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 EHR is still in its inception. However, the potential it offers, the deficiencies and gaps it fills, especially ensuring the security and confidentiality of health data, makes it the forefront to be adopted in the healthcare industry nowadays. Different kinds of researches have been carried out for the application of blockchain technology in securing 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 as a way of sharing 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 in [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 an 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.

Further research in [26] proposes the conceptual design for sharing personal continuous dynamic health data using blockchain technology, which is supplemented by cloud storage. The authors proposed using hash pointers to the storage location to solve the problem of sharing large size 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 several types of blockchain application research in healthcare, most of the available solutions focus on securing and sharing personal EHRs, failing to address the interoperability of different healthcare systems in securely exchanging patient EHRs. Hence, the motivation for this work. The novelty in our proposed solution is that it facilitates 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.

3 The Proposed Architecture

The proposed architecture, which focuses on the interoperability of different blockchain networks, is implemented on the Ethereum blockchain platform. The Ethereum blockchain features a smart contract, which is stored on the chain and keeps the agreement among consortium members. All participants run it. Fig. 1 shows a pictorial representation of the proposed architecture.

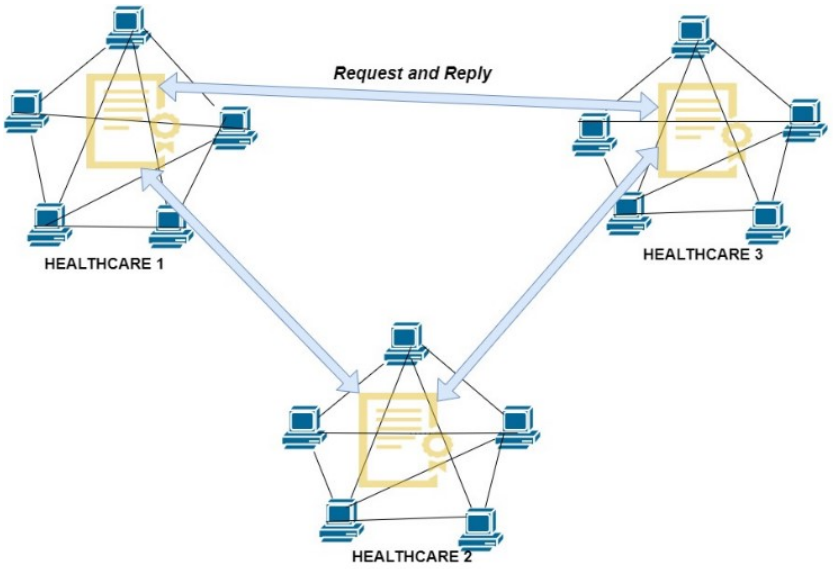

Fig. 1. The Proposed Architecture

The architecture comprises different healthcare systems running separate private blockchain network. In each private network, computers used for EHRs form nodes in the blockchain network. Each blockchain network is independent of each other and features a unique smart contract that is written according to the healthcare system's policies and health insurance portability and accountability act (HIPAA). The computers (also known as miners) in each network prepare, submit, and verify all transactions (patient's EHRs). The miners also run the consensus algorithm, thus validate transactions/blocks. In our previous works [29,30], we described how miners prepare, verify, validate, and retrieve stored transactions from a consortium blockchain network. In these past works, we focused on how cyberattack features are securely distributed among different nodes through the blockchain network. In this paper, miners in a healthcare network prepare, submit, verify, and similarly validate transactions as described in our previous works; however, unlike the previous work, which uses public-private blockchain networks, we set up a fully private blockchain network for each healthcare system.

In the current work, we focus on investigating a secured inter-healthcare EHRs exchange. In this implementation, the healthcare systems are assumed to keep and maintain patient health information on separate blockchain networks while we evaluate the interoperability's security. Each healthcare network contains miners and a smart contract already running on the chain. The miners prepare transactions, submit, and validate these transactions while the smart contract handles the transaction verifications. A transaction can be a patient's health information about to be stored into the blockchain network, requesting patient information from other healthcare or replies that carry the requested patient's information. We described how information could be stored and retrieved within a blockchain network in our previous works, in

this paper, we describe how our architecture carries out the formation of a patient's information request and reply across different blockchain platforms.

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

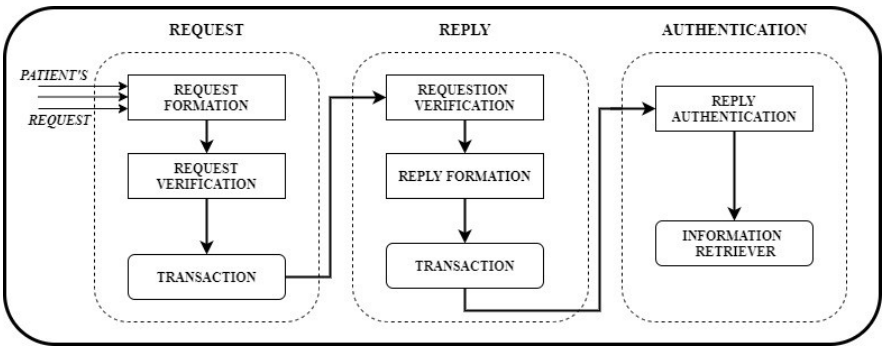

Fig. 2. Steps in the proposed architecture

3.1 Request

The request stage is subdivided into three categories: Request formation, Request verification, and transaction formation. The request is formed based on the information and permission from the patient. The request formation is necessary when the past medical history of a patient is needed for treatment. For example, a person that lives say in New York, USA, travels to London, UK. If the person had to visit the hospital for treatment, the past medical history must be retrieved from the New York hospital. The past medical history 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 miners. 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 also verifies the identity of the requester. The request is developed into an agreed-upon format and submitted as a transaction to the hospital's blockchain network. Apart from the submitted transaction, the miner (node) submits its information, which involves the requester's unique code, the MAC address, and the transaction address of the miner. The smart contract verifies the format of the transaction, the requester, and the miner's identities. The purpose of the verification is to detect and prevent all malicious activities on the transaction either by insider or outsider threats. Algorithm below describes the significant steps in the verification process. Since the blockchains communicate via smart contracts, each smart contract running on the blockchain networks contains the processes described in

algorithm1. For a request to be successful, it must agree with a standard format, the unique code of the requester must be in the authorized code sets, former healthcare must be in the table, miner information must be correct, and the public key of miner must verify its private key If any of these verification steps fail, the transaction is dropped, and smart contract returns failed request. A successful request is validated and attached to request blockchain. For more about validation, visit our previous works in [29 and 30].

```
program Verification (Request/Reply)
var   formatted request/reply; miner information;

begin
If Request;
      If     (request agrees with standard format) and
            (requester code in authorized code set) and
            (destination in look-up table) and (miner
            information is verified) and (public key
            verifies private key);

                  Validate transaction;
                  Return success;
      else;
                  Return fail;
                  Drop transaction;
      end;

 else;
      If    (reply agrees with standard format) and
            (reply source matches request destination)
            and (Verification information in respective
            sets);

                  Validate reply;
                   Return success;
      else;
                  Return fail;
                  Drop transaction;
      end;
  end;
 end.
```

3.2 Reply

After a successful validation process, the smart contract routes the request to the designated healthcare network based on the look-up table. The smart contract verifies the format of the received request and the requesting network. Algorithm below describes the verification of requests received by the healthcare network. For

a request to be successful, the format of the request must agree with a standard, source information must pass verification step, requested EHRs must be available in the healthcare network, and source public key must verify its public key. If any verification fails, the request is dropped, and the smart contract issues a failed request to the sending network. A successful request is validated and attached to the blockchain. Based on the required information, the miners compete to prepare a reply by retrieving the patient's EHRs from the blockchain network and preparing it for a transaction submitted to the blockchain for verification. The transaction (reply) and respective sending node are verified. A successfully verified reply is validated and attached to blockchain while routed back to the requester's network.

```
program Reply formation (Reply)
var   formatted request; Source information;

begin
If     (Incoming request agrees with standard format) and
      (S.I. in lookup table) and (Patient's EHRs in
      destination Healthcare) and (source public key
      verifies source private key);

            Validate transaction;
            Return success;
else;
            Return fail;
            Drop transaction;
end;

end.
```

3.3 Authentication

The requesting network verifies the sending network and the format of the received reply, as shown in verification algorithm above. When the verification process is successful, the transaction (reply) is validated and attached to the blockchain. The newly added block reflects on the ledger of every node in the network. Every blockchain node possesses a copy of this ledger. All blockchain nodes 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.

4 Result

We carry out the implementation of the proposed architecture in the lab. We set up two different blockchain networks (I and II) with each network comprising of three nodes. For each blockchain network, we use Solidity *v 0.6.2* implementation for smart contract and *geth v 1.9.0* for Ethereum. The smart contract is written as described above and mined into the blockchain network. A transaction (request) was prepared as explained in section III and submitted to the transaction in blockchain network I. We randomly generate ten-string long numbers to serve as the unique requester code. The MAC and transaction address of each miner, the format of a request and reply, and the requester's unique codes are written in the smart contract. Apart from this, a look-up table that stores information about the blockchain II is written in the smart contract. This smart contract is mined into the blockchain I. We write a similar smart contract (with the blockchain I information) into blockchain II's smart contract. We evaluate a preliminary result on the security analysis to demonstrate how the architecture detects and prevents threats from outsider and insider intruders within the blockchain network. We implement how the architecture detects an unauthorized node's attempt to submit a transaction to the blockchain network.

4.1 Security Analysis

4.1.1 Outsider Threat Detection

We analyze the security of the architecture against malicious transaction injection. We added a node (malicious node) that was not part of the blockchain to network I. Here, we assume that an attacker may find its way into joining the blockchain. The malicious node prepared a request transaction and submitted it to the blockchain network for verification. Although the transaction agrees with the standard, we observed a failed transaction notification contrary to the transaction address expected.

The transaction failed because the sender is not privileged to submit the transaction; hence, it fails the verification step. We further check if the transaction is validated and join to the chain by querying the blockchain using manually created transaction address. The result shows that the transaction is not chained to the network.

4.1.2 Insider Threat Detection

Here, we tested the security of the architecture against two typical ways a malicious insider can breach the patient's health record.

Multiple Requests. We implement a case where malicious insider compromised an authorized node and begins to send a large amount of what appears to be legitimate standard formatted request 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 mined because the frequency of receiving the same or similar transaction from the same node exceeds the threshold set in the smart contract. We persistently submit the same request from the same authorized node, and we observed that the miners stop mining after the sender was flagged to be compromised. The smart contract automatically drops all subsequent transactions from the same authorized node.

Unauthorized Retrieval of patient information. We implement a case with malicious insider attempts to retrieve patient information. It is assumed that an attacker is not likely to hold an authorized node in a compromised state for too long due to frequent security checks. Based on this assumption, an attacker makes all efforts to assess the information in the shortest time. The result showed that no information was returned because the node used is not privileged to retrieve the information. In the smart contract, information retrieval privilege is set for each node (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.

5 Conclusion

In this on-going research work, we propose a blockchain-based architecture that facilitates and secures inter-healthcare EHRs exchange. The proposed solution focuses on preparing a secured patient's EHRs request and replies to and from another healthcare system. In this implementation, each healthcare system is assumed to keep and maintain patient health information on separate blockchain networks while we evaluate the security of the interoperability between them. We evaluate the security of the architecture on the detection and prevention of malicious transactions within a healthcare system. The preliminary result shows that 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 :

- Detect malicious replies or requests coming for another healthcare system.

- Investigate how it protects against more insider threats scenarios
- Evaluate the response time

References

1. J. clement (2020), Number of U.S. data breaches 2013-2019, by industry, https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/
2 Heather Landi (2020), Number of patients records breached nearly triples in 2019, https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats
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, http://bitcoin.org/bitcoin.pdf

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.