Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 175 (2020) 615–620

Procedia Computer Science

www.elsevier.com/locate/procedia

The 6th International Workshop on Cyber Security and Digital Investigation (CSDI)
August 9-12, 2020, Leuven, Belgium

Blockchain and Smart Healthcare Security: A Survey

Noshina Tariq[a], Ayesha Qamar[a], Muhammad Asim[a], Farrukh Aslam Khan[b,*]

[a] *National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan*
[b] *Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11653, Saudi Arabia*

Abstract

The Internet of Things (IoT) has penetrated its roots in almost every domain of life. Smart healthcare is one of the major domains that extensively uses IoT infrastructures and solutions. IoT-based smart healthcare systems have immensely added value to the healthcare domain with the use of wearable and mobile devices. This leads to a substantial use of health data sharing for the improved, accurate, and timely diagnosis. However, smart healthcare systems are highly vulnerable to several security breaches and various malignant attacks, such as privacy leakage, tempering, forgery, etc. Recently, the blockchain technology emerged as a propitious solution against such breaches and challenges. This paper presents an up-to-date survey on different challenges and open issues faced in smart healthcare due to the traditional security measures along with the security requirements of such domains. It also amalgamates the potentials of blockchain technology as a promising security measure, highlights potential challenges in the healthcare domain, and provides an analysis of different blockchain-based security solutions.

Keywords: Blockchain; Smart healthcare; Security; Privacy

1. Introduction

With the emergence of the Internet of Things (IoT) and wearable technology, many opportunities as well as challenges have escalated in the healthcare domain. Inter-connectivity of smart devices (e.g., wearable devices and vital monitoring sensors) constitutes massive health-related data. Thanks to the cloud computing and big data analytics for deriving valuable and useful insights out of these data for effective decision making. The extracted data could also be used by hospitals and medical institutions so that they could connect with the existing Electronic Health Record (EHR) for improved health observation, disease diagnosis, and timely treatment [1]. In addition, it may also help health insurance companies in making in-depth strategic policies for customers. In 2009, U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act reserved approximately 36.5 billion dollars to invest in

[*] Corresponding author. Tel.: +966-11-4697341 ; fax: +966-11-4695237.
E-mail address: fakhan@ksu.edu.sa

10.1016/j.procs.2020.07.089

health organizations to use EHR systems instead of the traditional methods to manage data [2]. Nowadays, the EHR market is highly valued, which may be counted in the figure of tens of billions of dollars [1]. However, sharing health data needs a secure and trusted infrastructure as there exists many risks related to privacy, security, and interoperability. Firstly, health data have huge privacy-sensitivity; particularly as more and more data is being stored on the cloud. Therefore, the challenges of revelation and leakage of confidential data are increasing. Secondly, the centralized architectures are widely used in the current systems as well as in the security mechanisms. Hence, it is challenging to effectively integrate interoperability among healthcare systems, which are distributed in deployments. In addition, it is also a major challenge that users have less access to the private health data [3]. Keeping in mind the concept of self-ownership along with the increased mobile platform adoption and portable computing devices, it is inevitable to develop a newer release of EHR systems that would ensure control of user access and preservation of security in a much distributive yet effective way.

It is of much significance that such systems should own the ability to share data in an efficient and secure manner [4] [5] [6]. In addition, they must also provide greater access control, privacy, and anonymity to the respective individuals. If there is no/less security, privacy, and trust handling, the individuals will become reluctant to provide their important information or they may avoid seeking the treatment [7]. Currently, many health data systems rely on a single party for the management of confidential health data, which is highly prone to single-point-of-failure. However, the technology of blockchain could change this reliance due to its distributive nature. It provides the ability to overcome failure and attacks (as discussed in later sections) in a distributive and immutable way. In addition, it also provides a record for the ownership of data and its authenticity [1] [8]. It relates to the pseudo-anonymity in addition to the public key infrastructure (PKI) while retaining the privacy of the users [7]. The use of blockchain technology in healthcare as well as in its research is detailed in [9]. The work supports the use of blockchain technology in the healthcare domain, which also includes preservation of privacy for prediction modeling, increasing large scale interoperability among institutions, invariability of health history records, improvement of health assurance process, interchange of health data, artificial intelligence supporting healthcare models, management of identity, strategies of earning revenue, and data record [10].

This survey provides an integrative study covering security requirements along with challenges and open issues in patients' information sharing, loopholes in existing solutions, and privacy pledge regarding blockchain add-on in smart healthcare as compared to monotonic available state-of-the-art surveys. To provide a baseline for other researchers, it also filters out the booming trends in the said area. It highlights that apart from other security solutions, blockchain may provide a decentralized and scalable solution to meet the growing needs of the smart healthcare domain. The main contributions of this paper include a concise analysis of essential security requirements of smart healthcare systems. We also discuss the benefits of blockchain adoption in security as well as its efficacy in the smart heathcare domain by scrutinizing different blockchain-based solutions in securing healthcare data against potential security breaches. In addition, the survey also highlights different challenges of the usage of blockchain in this domain.

The remainder of the paper is organized as follows: Section 2 details the security requirements of smart healthcare systems. Section 3 presents blockchain and its applications in the healthcare domain. Finally, Section 4 concludes the paper with possible future directions.

2. Smart healthcare security requirements

The IoT notion in the medical realm includes validation, automatic information compilation, and discerning. IoT-enabled smart healthcare systems deal mostly with patients' personal information and findings. This data is highly prone to malicious attacks if not secured with advanced and formidable security measures [11]. Unfortunately, some of the smart devices and sensors used in the smart healthcare domain are resource-constrained (having low processing and storage capabilities). Consequently, supporting security protocols cannot be integrated in them [12] [13]. Furthermore, the nature of such devices is mobile and may need public network connections, such as hospitals, homes, offices, etc., which further add to its vulnerability. With the exponential increase in connected IoT devices, designing dynamic and stable security mechanisms is a challenging task [14] [15]. For instance, the development record of patients' health situation is confidential, and it needs a safeguarding method to avert the information dispersal to an unsanctioned group. By functioning in this way, no one can observe and manipulate the data or pass a faulty patient health record. It also prevents a doctor from performing error in handling the patients. If no safety procedure is adopted, the medical practitioners may give incorrect medication or furnish wrong nursing to their patients [16]. For example, modifications to a blood examination report might aggravate a patient's situation because of transfusing incompatible blood during the blood transfusion process. The important security requirements in the IoT-enabled healthcare domain are outlined in Table 1.

Table 1. Smart healthcare security requirements.

Requirement	Description
Confidentiality	Ensures that health data is preserved and cannot be accessed by unauthorized entities. In IoT domain, a number of connected devices, applications, and parties are part of healthcare domain making data hampered to improper diagnostics [13].
Integrity	Refers to the correctness of health data, either gathered or disseminated to the authorized entities without any fabrication or modification [17]. Modified and fabricated data may also lead to improper diagnosis and hazardous consequences.
Availability	For timely diagnosis and treatment, healthcare data must be available as and when required without delays [18].
Ownership	Ensures that the health information and data captured belongs to a particular entity (the creator) with all rights. This characteristic restricts unauthorized access and misuse [19].
Privacy	Holds that the health data and information is available to authorized users only. For example, patients' data and information is not provided to any third party without their permission. Privacy also ensures that the data will be secure in transit or in storage.
Authenticity	Refers to the truthfulness of the requesting entity, which means only the authentic party may access or modify the health data [19].
Non-repudiation	Ensures neither user nor patient can deny the provided data. It may be handled by digital signatures and encryption [20].
Auditing	Ensures the overall credibility of a healthcare application. It refers to maintain log of all the transactions (captured or modified) [21].
Access Control	Ensures controlled and legitimate access to the health data and information either public or private [19].
Data Freshness	It makes sure that the data is not inconsistent and is up-to-date. To ensure this property timely, data availability must be ensured. Delays may make unwanted and calamitous effects on diagnosis and patients' life [22].
Anonymity	Refers to the privacy of patients' identity, concealing from public and unauthorized entities. It makes sure that the data stored in such a way ensures anonymity of patients' identification [23].
Secure Data Transit	It makes sure that the data in transit is also safe and is not being altered or observed. It ensures that the adversary will not have access to the data in transit, nor it can inspect or alter it [14].

3. Blockchain

Blockchain technology has been exhaustively researched in the past few years. Satoshi Nakamoto [24] introduced the concept of blockchain as the supporting mechanism of the digital cryptocurrency called Bitcoin. The fundamental concept of the blockchain technology gives a basis for cooperation between unknown and untrustworthy things, while also corroborating the disseminated features of mobile (smart health) devices, lacking the need of a central security and authentication authority, as in the current cloud computing architectures [25]. This main technology relies in an immutable "public ledger", which is a record of data shared among all the participants. This public ledger contains blocks of data, linked together with the use of a cryptographic hash key. The linking process (also known as consensus) is called Proof of Work (PoW) [8]. Both the ledger and the consensus mechanism are innately impervious to data manipulation. The block data cannot be altered post-fact, because this invalidates previous block hashes in the blockchain and breaks the consensus among nodes. The use of the blockchain technology allows Bitcoin's public distributed ledgers to make transactions of digital money inexpensively and securely without a third party that would verify the transaction and avoid the perennial "double spending" issue [25]. A smart contract is executed as a storage process whenever a transaction is initiated. The key characteristics of blockchain technology includes decentralized control, data transparency and auditability, distributed information, and security from malicious actors [8] [25].

3.1. Blockchain and smart healthcare

Serious cyber attack concerns have emerged in healthcare services during the past few years. A record number of cases have been reported in the year 2019, where Health Insurance Portability and Accountability Act (HIPAA) breaches reached to 418, and a total of 34.9 million US citizens had their protected health information (PHI) compromised in that year [26]. The existing infrastructure is not capable of providing security against such data breaches, which can ultimately question the privacy and security of patients' health information. The presently implemented models of smart healthcare records open another window towards a problematic scenario, i.e., the patients' data being in the custody of health organizations, leaving patients' information at stake, and causing inefficient data delivery towards patients' healthcare. For example, just because the information about a patient's health is not sent from one service provider to the other in time, the patient's treatment might get delayed. EHR has such limitations practically, which can be overcome by using blockchain. Recently, blockchain has been adopted by several government, private, and public-private partnered projects [27]. Blockchain's potential benefits in the field of healthcare were witnessed when the US Food and Drug Administration (FDA) and IBM Watson Health focused on a blockchain framework to protect data related to oncology [28]. Blockchain allows data collection from various sources and saves that data in the transaction audit log, which ultimately helps in keeping track of accountability and transparency of data at the time of data exchange. It is believed by FDA and IBM that blockchain has the capability to support data exchange collected from various sources with the consensus of patients and the terms mutually agreed on [27]. Presently implemented models have the dependency on passwords, which may contain secret data that has to be exchanged and usually stored on unreliable and less secure clouds [14]. This caused numerous well-known cyber accidents, the most famous of which was the one that took place in 2014, when hackers intruded into US Health insurer Anthem's servers and the sensitive information of about 80 million people (patients and employees) got stolen [27]. It is also of great importance that the healthcare data access must be handled with precautions. Similarly, standardized auditing is inevitable for guaranteeing data integrity. Blockchain reduces the chances of such disastrous breaches and ensures data integrity, anonymity, and resilient storage. In addition, single-point-of-failure is also mitigated as this model stores data in a distributive way.

Table 2. Blockchain-based security solutions in smart healthcare systems.

Reference	Issues Addressed	Blockchain Solution	Advantage
[29]	Access control, data obfuscation	Ethereum-based smart contracts and cryptography with no monetary-based mining incentives	Data ownership, integrity, and scalability
[30]	Privacy leakage, single-point-of-failure, and sybil attack	Privacy preserving, data encryption, access control, and key management	Privacy, accountability, and on-demand rescission
[31]	Privacy, eavesdrop, and intrusion attacks	Distributed web platform, access control	Pseudonymity, privacy, integrity, accountability
[32]	Privacy issues	Private blockchain and consortium blockchain	Access control, auditing, privacy preservation, secure search, and time-controlled rescission
[33]	Real-time patient monitoring security	Permissioned and consortium-managed blockchain	Confidentiality, availability, immutability, traceability, privacy, and transparency
[34]	Data leakage, malicious operation, and dishonest user	Customised search index-based blockchain	Fair analysis, reliable search results, confidentiality, integrity, anti-tampering, and traceability
[35]	Data integrity and repudiation issues	Blockchain-based notarization	Data integrity, non-repudiation, data versioning
[36]	Data sharing, scalability, and Quality of Service (QoS) issues	Blockchain-based smart and secure Healthcare system (ssHealth)	Scalabilty, data sharing, QoS, efficient, remote monitoring
[37]	Privacy and anonymous information sharing issues	Two-layer consortium blockchain along with a new consensus algorithm (MBFT)	Privacy protection, tamper-resistance, high fault tolerance and efficient transaction handling
[38]	Single-point-of-failure, man-in-the-middle attack, denial of service, and data sniffing attacks	RHM solution based on a public blockchain	Privacy preserving, identity management, security, immutability, efficient message delivery times

The information that authenticates a subject is a major challenge in identity as well as in access management. An example could be a username, password, and thumb-print used for verification of a person. On the other hand, authentication of an identity based on blockchain technology makes use of private keys, which are used to sign every transaction. Another issue is the missing data auditing trail. It also covers the area of user preferences and a consent of his/her data usage. Blockchain supports data auditing trail, i.e., a complete log of electronic data creation, changing, and removing is maintained. Authorization to perform actions by different stakeholders is also a challenge in smart healthcare systems. A policy assigns the rights of access to data for each stakeholder. However, mostly, the patients do not have self-ownership of their data. Thanks to the blockchain technology that supports authorization, legitimate access to data, and self-ownership of patients on their data. Last but not least, efficiency also plays an important role in challenges faced in the said domain. Inefficiency in administration, logistics, and in delivery of services results in cost and time overheads and less advantages are achieved [39]. The reasons could be the inefficient exchange of data and flaws in policy making. In addition, monitoring and logging of every access to EHR must be ensured to forbid non-monitoring of access to sensitive healthcare information. However, this milestone is somewhat difficult to achieve for traditional healthcare systems, as most of the health organizations do not follow the mechanism of strict authorized access. Moreover, the infrastructure of patients' databases does not contain good security requirements. Blockchain can be a solution to these issues that may lead to solving a general problem of privacy and authentication. It also supports data auditing and time-stamping that could help patients to identify modifications in data with respect to time as well as identity of the person who modified it. In a blockchain scenario, patients can permit third parties to access data, however, third parties cannot store it. To conclude, blockchain-based solutions are higher-ranked than existing traditional systems. Table 2 summarises some blockchain-based security solutions in smart healthcare systems along with their advantages.

Although blockchain gives an add-on to EHRs, it still faces certain challenges that contribute to limitations of this field. However, engaging blockchain in this filed is packed up by educational barriers instead of technical ones [27]. Healthcare providers may face certain roadblocks due to access control and ownership factors that could hinder them to adopt blockchain. In addition, psychological challenges faced by healthcare organizations should be admitted and tackled to address issues of security, privacy, trust, and integrity. Traditionally, most of the healthcare providers are the only owners of the patients' information within their organizations [40], which needs to be changed. However, it is a difficult task to change the norm. On the other hand, old people or patients with mental health problems are not able to manage their medical records, and eventually cannot use blockchain for access control and self-ownership, for example. Moreover, there exist some privacy laws for IoT-enabled healthcare data, e.g., HIPAA of 1996 that should be applied strictly in this domain [41]. If proper encryption is applied to patients' data along with an appropriate control policy, the two factors can contribute a lot in trust management in this domain. Furthermore, scalability issues also exist due to increasing size of generated data with time. By adopting blockchain, every participating node in the network holds the complete medical record of a patient, which could lead to the problems of bandwidth usage and data storage [42].

4. Conclusion

IoT-enabled smart healthcare systems are prone to critical security threats and challenges. To mitigate these threats and challenges, it is needful to understand the security requirements of such systems. The traditional security mechanisms do not cater for all the security requirements of the IoT-enabled smart healthcare system due to less scalability, higher cost, single-point-of-failure, and resource-constrained nature of the IoT devices. Recently, blockchain transpired a new era of security and privacy in the healthcare domain. In this study, we addressed the security requirements of IoT-enabled smart healthcare systems along with the application of blockchain-based security solutions. We discussed how blockchain-based solutions can overcome different security issues in an efficient, distributive, and scalable way. In addition, we also highlighted the challenges of blockchain deployment is this infrastructure. In future, we aim to expand our study to an in-depth analysis of the authentication mechanisms to design an efficient blockchain-based identity authentication mechanism.

References

[1] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), IEEE, 2017, pp. 468–477.

[2] R. O. Jr., The Machinery Behind Health-Care Reform, https://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051503667.html, [Online; accessed 27-May-2020] (2020).

[3] L. J. Kish, E. J. Topol, Unpatients—why patients should own their medical data, Nature biotechnology 33 (9) (2015) 921.

[4] A. Ali, F. A. Khan, A broadcast-based key agreement scheme using set reconciliation for wireless body area networks, Journal of medical systems 38 (5) (2014) 33.

[5] F. A. Khan, A. Gumaei, A. Derhab, A. Hussain, A novel two-stage deep learning model for efficient network intrusion detection, IEEE Access 7 (2019) 30373–30385.

[6] N. Tariq, F. A. Khan, Match-the-sound captcha, in: Information Technology-New Generations, Springer, 2018, pp. 803–808.

[7] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–5.

[8] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for iot systems, Cluster Computing (2020) 1–21.

[9] L. Linn, M. Koo, Blockchain for health data and its potential use in health IT and health care related research, ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States (2016).

[10] T. Hardin, D. Kotz, Blockchain in health data systems: A survey, in: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, 2019, pp. 490–497.

[11] Z. Maamar, E. Kajan, M. Asim, T. Baker Shamsa, Open challenges in vetting the internet-of-things, Internet Technology Letters 2 (5) (2019) e129.

[12] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, T. Baker, A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot, Journal of Parallel and Distributed Computing 134 (2019) 198–206.

[13] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A Mechanism for Securing IoT-enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks 8 (1) (2019).

[14] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, Sensors 19 (8) (2019) 1788.

[15] N. Tariq, M. Asim, F. A. Khan, Securing scada-based critical infrastructures: Challenges and open issues, Procedia Computer Science 155 (2019) 612–617.

[16] F. A. Khan, N. A. H. Haldar, A. Ali, M. Iftikhar, T. A. Zia, A. Y. Zomaya, A continuous change detection mechanism to identify anomalies in ecg signals for wban-based healthcare environments, IEEE Access 5 (2017) 13531–13544.

[17] H. Wang, K. Li, K. Ota, J. Shen, Remote data integrity checking and sharing in cloud-based health internet of things, IEICE TRANSACTIONS on Information and Systems 99 (8) (2016) 1966–1973.

[18] A. Strielkina, V. Kharchenko, D. Uzun, Availability models for healthcare iot systems: Classification and research considering attacks on vulnerabilities, in: 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2018, pp. 58–62.

[19] S. F. Aghili, H. Mala, M. Shojafar, P. Peris-Lopez, Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot, Future Generation Computer Systems 96 (2019) 410–424.

[20] Y. Al-Issa, M. A. Ottom, A. Tamrawi, ehealth cloud security challenges: A survey, Journal of healthcare engineering 2019 (2019).

[21] M. Talal, A. Zaidan, B. Zaidan, A. Albahri, A. Alamoodi, O. Albahri, M. Alsalem, C. Lim, K. L. Tan, W. Shir, et al., Smart home-based iot for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review, Journal of medical systems 43 (3) (2019) 42.

[22] F. T. Jaigirdar, C. Rudolph, C. Bain, Can i trust the data i see? a physician's concern on medical data in iot health architectures, in: Proceedings of the Australasian Computer Science Week Multiconference, 2019, pp. 1–10.

[23] R. Khan, X. Tao, A. Anjum, T. Kanwal, A. Khan, C. Maple, et al., θ-sensitive k-anonymity: An anonymization model for iot based electronic health records, Electronics 9 (5) (2020) 716.

[24] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, [Online; accessed 15-June-2020] (2008).

[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering 30 (7) (2018) 1366–1385.

[26] H. Greevy, HIPAA breaches in 2019: A year in review, https://www.physicianspractice.com/hipaa/hipaa-breaches-2019-year-review, [Online; accessed 28-May-2020] (2020).

[27] N. Kshetri, Blockchain and electronic healthcare records [cybertrust], Computer 51 (12) (2018) 59–63.

[28] L. Mearian, IBM Watson, FDA to explore blockchain for secure patient data exchange, https://www.computerworld.com/article/3156504/ibm-watson-fda-to-explore-blockchain-for-secure-patient-data-exchange.html, [Online; accessed 28-May-2020] (2020).

[29] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable cities and society 39 (2018) 283–297.

[30] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet of Things Journal 6 (5) (2019) 8770–8781.

[31] A. Al Omar, M. S. Rahman, A. Basu, S. Kiyomoto, Medibchain: A blockchain based privacy preserving platform for healthcare data, in: International conference on security, privacy and anonymity in computation, communication and storage, Springer, 2017, pp. 534–543.

[32] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, Journal of medical systems 42 (8) (2018) 140.

[33] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of medical systems 42 (7) (2018) 130.

[34] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Generation Computer Systems 95 (2019) 420–429.

[35] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, E. Kaldoudi, A blockchain-based notarization service for biomedical knowledge retrieval, Computational and structural biotechnology journal 16 (2018) 288–297.

[36] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, A. Refaey, sshealth: Toward secure, blockchain-enabled healthcare systems, IEEE Network (2020).

[37] M. Du, Q. Chen, J. Chen, X. Ma, An optimized consortium blockchain for medical information sharing, IEEE Transactions on Engineering Management (2020).

[38] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere, F. Antonelli, A decentralized peer-to-peer remote health monitoring system, Sensors 20 (6) (2020) 1656.

[39] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, F. A. Khan, Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security, Sensors 19 (14) (2019) 3119.

[40] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data, in: Proceedings of IEEE open & big data conference, Vol. 13, 2016, p. 13.

[41] HIPAA, The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html, [Online; accessed 28-May-2020] (2020).

[42] L. A. Linn, M. B. Koo, Blockchain for health data and its potential use in health it and health care related research, in: ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016, pp. 1–10.