Third International Conference on "Materials, Computing and Communication Technologies"
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

e-Health Care Management Systems and its Decentralized Environment using Blockchain

[1] Gajanan P. Arsalwad, [2]Dr. Sohel A. Bhura
[1,2]Babasaheb Naik College of Engineering, Pusad, Maharashtra, India

Article Info
Volume 8, Issue 7
Page Number : 220-228

Publication Issue :
May-June-2022

Article History
Accepted: 01 June 2022
Published: 20 June 2022

ABSTRACT

When it comes to the kind of work that falls under this category, there is no room for taking any risks whatsoever. The health care industry is an especially delicate one in which every decision must be made with the utmost caution. The data of patients are transferred from one institution to another as the primary focus of the BC technique in the health care industry. As a result of the fact that many concerns either avoid doing it or do it in an unreliable manner, there is a significant amount of uncertainty regarding the dependability of the data generated by a concern. Therefore, using the BC technique when sharing data about health care will result in the creation of trust regarding the data that is shared. It is a question worth a billion dollars whether people will have access to health care records in this global arena. This is due to the fact that maintaining the data's integrity is essential in order to keep track of patients or to develop new solutions to diseases by maintaining a record of the health history. This will also help researchers who are working in a particular field to come up with solutions to recurrent health problems.

Keywords : Healthcare, blockchain, Decentralized, Environment.

I. INTRODUCTION

It has been suggested that the Internet of Things (IoT) [1] should serve as the basis for the intelligent and healthy cities and regions of both today and the future [2]. There are blockchain solutions that are geospatially enabled that make use of a crypto-spatial coordinate system in order to provide an immutable geographical context, something that standard blockchains do not have [12]. These geospatial blockchains not only record the precise time that an entry was made, but they also require and validate its associated proof of location. This not only enables accurate spatio-temporal mapping of events that occur in the physical world, but it also enables a wide variety of application possibilities that are based on smart cities and the Internet of Things [3]. In the not-too-distant future, it is anticipated that there will be an increase in demand for Internet of Things (IoT) devices and applications that can negotiate with, and pay one other for secure, safe operation and services.

Some examples of these Internet of Things devices include mobile and wearable devices that can be used to pay for public transportation [4], as well as autonomous connected devices and vehicles for smart city emergency/disaster response, such as a drone defibrillator, or a drone for the delivery of ordered medicines and medical supplies [15, or a self-driving ambulance car, or helicopter. [Citation needed] The blockchain-powered, distributed peer-to-peer apps that are powering these smart devices, drones, and vehicles would eliminate the "middleman" and the dependence on third-party centralised providers, for navigation and other geospatial data. Additionally, this would reduce the likelihood of an IoT-powered autonomous vehicle being hacked and driven to the wrong location. Interoperability [7], security [8], and privacy, jurisdictional difficulties [9], and the need to develop viable and sustainable economic models of deployment are some of the obstacles that blockchain technologies are currently experiencing today. At the conclusion of this chapter, a short discussion of these difficulties is going to be provided.

II. LEVELS OF HEALTHCARE MANAGEMENT

The provision of medical treatment is predicated mostly on the collaboration of skilled professionals working in interdisciplinary teams. Teams of medical professionals, therapists, psychologists, and dentists, as well as public health practitioners and community workers, collaborate on the delivery of preventative and rehabilitative health services as part of this initiative. Even while all healthcare practitioners strive to accomplish the same overarching aim, they may be broken down into one of three distinct groups.

Primary healthcare refers to the provision of medical services by medical professionals who are the patients' first point of contact and consultation within the healthcare system. This category offers the greatest amount of flexibility for persons of all ages, from all different socioeconomic situations, and living with a variety of chronic conditions. As a result, the primary healthcare practitioner is anticipated to possess comprehensive expertise in a variety of domains. The provision of primary healthcare is often important to the community at large.

Secondary healthcare refers to the provision of intensive treatment for a disease that is severe but only expected to last for a limited amount of time. It is possible to think of it as being synonymous with the emergency department of the hospital. Patients are often obliged to see a primary practitioner for a referral before consulting secondary care. This need is based on the policies and organisation norms that govern healthcare organisations.

Tertiary healthcare is a specialist unit that is mostly consulted on the basis of referrals from primary or secondary care. This segment of the healthcare industry is known as tertiary care. Because treatment in this area demands a higher level of attention and more time, patients are often only assigned here when it is anticipated that they may suffer from chronic conditions.

III. ISSUES AND CHALLENGES

In today's healthcare system, one of the most persistent challenges is figuring out how to boost patient satisfaction while simultaneously lowering expenses and expanding revenue [10]. Even if a great number of technological solutions have been developed in order to address the issues plaguing the sector, there are still a great deal of obstacles to overcome in terms of protecting users' privacy and safety. Inefficiency still remains in

the sector, despite the fact that various changes have been made, and this may occasionally lead to major hazards to the lives of the patients involved [11]. In spite of the fact that the introduction of wire-free sensor networks in the healthcare industry is becoming more widespread [12], the uses of blockchain technology in the healthcare sector are going to cause a revolution in the way that the industry functions.

In [13] Because healthcare firms collect extremely sensitive patient data, the sector is a primary target for cybercriminals. Due to the fact that healthcare companies are notoriously sluggish to react to problems of this kind, this issue will continue to plague the industry. The presence of centralised systems that are responsible for data maintenance makes the data more susceptible to being attacked over the internet. When a data breach occurs, not only does it result in the disclosure of important patient information, but it also constitutes a violation of the policies and procedures of the organisation, which in turn creates substantial risks for both the business and the patients who are involved. As a full-time solution, healthcare institutions should use a system that is not only more resilient but also safer in nature. This is in addition to taking measures to avoid cyber crime.

Interoperability refers to the capacity of disparate information systems and software technologies, such as Electronic Health Records (EHRs), to interact with one another and share data [14]. It is essential, for the purpose of providing appropriate care and safety to people and communities [15], to make it possible for the information to collaborate both inside and beyond the organisational boundaries. For instance, interoperability enables healthcare providers to securely communicate patient data with one another regardless of the locations of the parties participating in the exchange [16]. This is possible regardless of the trust relationship that exists between the two parties.

It is very necessary to share data in a secure manner in order to offer patients with appropriate collaborative therapy and care. Data sharing helps to improve diagnosis accuracy [17] by gathering confirmations and opinions from a variety of specialists in the field. Inefficiencies and mistakes in the treatment plan and medicines will be avoided as a result of this as well [18]. Patients are required, under today's healthcare systems, to compile and share their medical records with their doctors, either in the form of paper copies or electronic versions. This is despite the fact that data sharing is an extremely important aspect of the healthcare industry. This procedure is ineffective since it is sluggish, unsafe, could be missing certain steps, and does not provide context. The inefficient process for exchanging data is the root cause of a lack of trust among providers, as well as a lack of interoperability across the many health systems and apps in use today.

The volume-based to the value-based paradigm change is now taking place within the healthcare business. In the past, the providers were given financial incentives to increase the number of treatments they provided since reimbursement was contingent on the total number of patient encounters. Care that is oriented on the patient and of the highest quality may be made easier via the implementation of value-based medicine. Patients are included in the decision-making process and given accurate information under this method. It also makes it possible for the data to be gathered on the digital platform and makes it simple for them to access it, which helps reduce the amount of information that is fragmented and inaccurate as a result of communication [19].

Patients should be able to choose to what extent they are willing to share their information and should have the ability to control when and with whom their medical data are shared. In addition, it is necessary that patients have the ability to control when and to whom their medical data are being shared. However, the healthcare systems that are in place now do not provide such flexibility. Once a certain practitioner gets their hands on a patient, the patient will be under their care indefinitely. The patient does not have the ability to

change the access that has been granted to a specific provider under the existing system[20]. Therefore, if a patient sees a number of different providers over the course of his lifetime, his private medical information will be stored permanently at a number of different locations. This only causes a single supplier who is not current with the most recent security procedures, therefore the danger of data theft is increased even if it is just one provider[21].

The medical data include a vast quantity of information stored in a variety of forms, such as photographs and scan results, which may be sent among a variety of stakeholders. Because of the limitations imposed by the firewall settings or the bandwidth, it is impossible to exchange such a vast collection of data via an electronic platform[22]. In addition, there is not a centralised platform or infrastructure that can collect, store, and exchange the data that comes from a variety of sources. On a consistent basis, massive amounts of data are created; yet, this information is dispersed among a variety of sources and parties, such as payers, patients, and providers[23]. As a result, there is no central access point for healthcare professionals, making it impossible to improve the quality of care patients get.

IV. DECENTRALIZED ENVIRONMENT

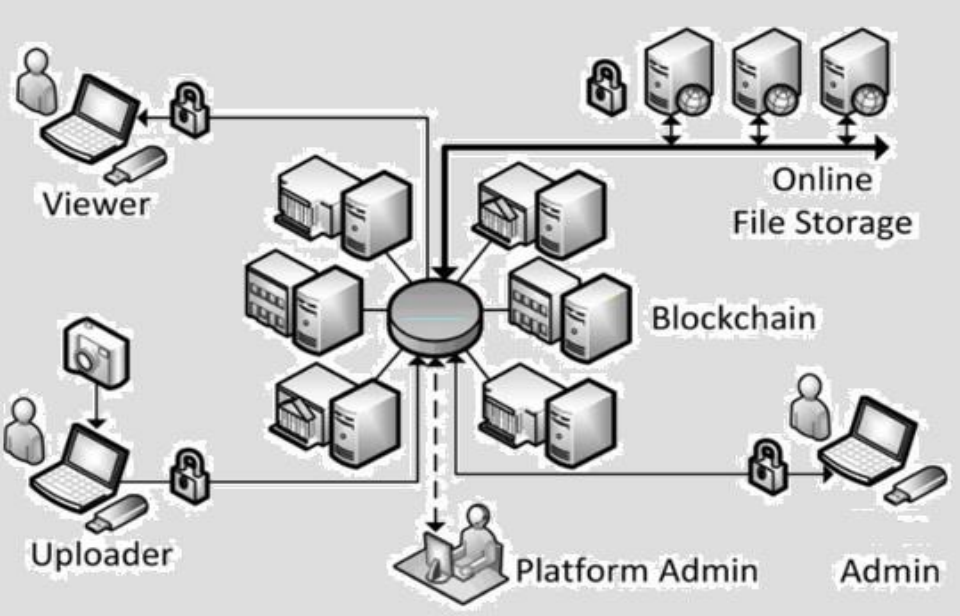

Figure 1. Decentralized Environment

In their pioneering work [38], Haber and Stornetta were the first to show the concept of blockchain technology via their study. [38] They proposed a chain of blocks that was both cryptographically protected and able to store data in a manner that prevented any kind of tampering from being feasible thanks to the combination of timestamps. The concept was advanced by using the principles of Merkel Tree in order to enhance the efficiency and capacity for storage offered by the blockchain system [39]. However, the notion of blockchain for bitcoin didn't emerge until 2008, and it wasn't until after that year that the technology really took off and advanced at a rapid pace. The research on bitcoin and the technology that underpins it, known as blockchain, was given by a person going by the name Satoshi Nakamoto [6], the identity of whom is not yet known. He went on to explain how the decentralised feature of blockchain technology, which means that nobody will

ever be in charge of anything, contributes to the enhancement of digital trust. The term "blockchain" refers to a distributed ledger that was created by Satoshi Nakamoto in 2008 as the foundational idea for the digital currency bitcoins [6]. Transactions between two parties may be carried out directly using blockchain technology and cryptocurrencies, eliminating the need for a third party to serve as a middleman in the process. The immutability, sequence, and integrity of the related transactions may all be guaranteed with the use of cryptographic features that are assisted by blockchain [40]. This technology was developed with the intention of removing the need for intermediate parties so that the interests of the parties engaged in a transaction could continue to be protected while the expenses associated with using intermediary parties could be reduced. The elimination of the need for centralised authorities in decentralised applications is perhaps the most immediately apparent advantage offered by blockchain technology. When there are two or more parties engaged in a transaction, the risk of a transaction stalling due to a single point of failure is reduced thanks to blockchain technology, which eliminates the need for centralised authorities. Therefore, the transaction is improved since it avoids the centralised third party, which also results in a reduction in the cost of the transaction. A method known as consensus is used in order to eliminate any potential for disagreement. The comparison between centralised and decentralised systems is shown in the next paragraphs. Even if there are a number of different ledgers, all of the records are kept in a single location when using a centralised system. The condition of the ledger is kept up to date by System ABC, as shown in Figure 10.2. In the event that there are any disagreements about the current status of the ledger, the central authority ABC is approached for ultimate adjudication. On the other hand, in a decentralised system, there is only one ledger, but each ledger stores an identical copy of the records and provides equal access to the information it contains. The term "consensus" refers to the state of the ledger at which all of the nodes in the network are in agreement. There are a variety of approaches that may be used to reach a consensus. The use of blockchain technology has expanded outside the realm of cryptocurrencies due to its transparent and auditable capacity to record and store transaction histories [41]. This is despite blockchain's current preeminence in the cryptocurrency space. The disruptive nature of this technology may be attributed to blockchain's inherent capacity to include smart contracts. Smart contracts are nothing more than a logical code that is run through blockchain technology. These codes mimic the standard contracts that are used. A smart contract not only governs the circumstances that need to be satisfied, but it also manages the behaviour that has to occur in the event that these requirements are not met. As a result, they may be used to automate a variety of tasks, including payments, paperwork, and so on. The capacity of smart contracts to do away with the need for middlemen and to build confidence between the parties involved in a transaction has caused a disruption in the use of technology in many different fields [41].

V. Analysis of Decentralized Environment

The performance of the blockchain, which should be checked for all factors that are relevant to the network's latency, is the third component that has to be evaluated. The latency of the network is determined by many factors, including the size of the block, the number of nodes that are participating, the anticipated size of the transaction, and the access time of the queries. Testing for performance should determine whether controls, such as auto-scaling, are required to make use of a cloud environment while dealing with chaotic conditions.
In conclusion, it is necessary to conduct security tests on blockchain against many types of threats.

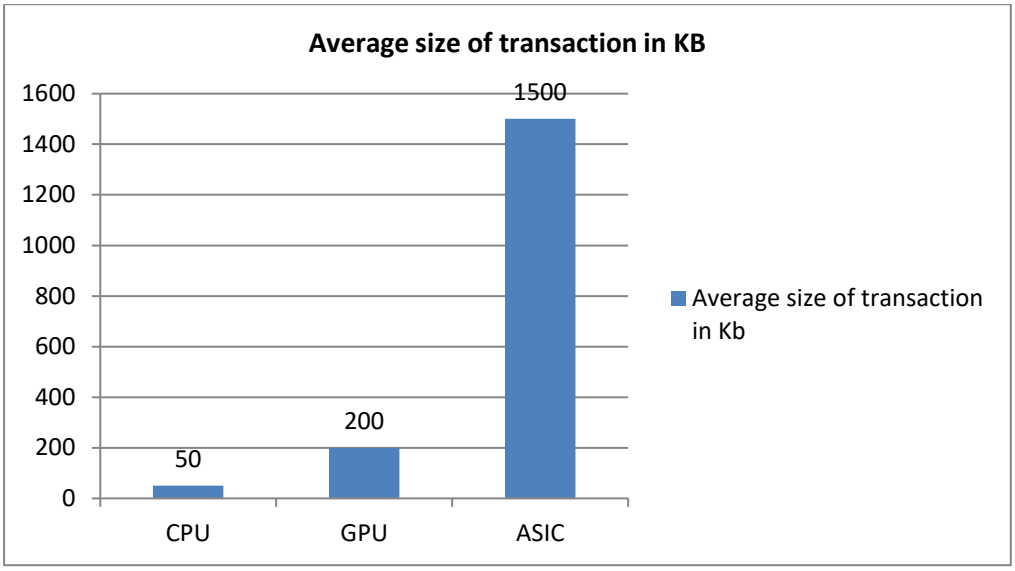

Figure 2. Transaction rate in Blockchain System

Another experiment that we have carried out in order to gain the scalability, flexibility, and resilience of the system with the same machine capacity that we had examined in the previous experiment, but now we have attempted with 20,000 transactions we create result in order to see what happens. Due to the increased number of transactions, we now need more processing time to get the desired outcomes; nevertheless, this delay may be seen as a hidden parameter that indicates how reliable our system is.

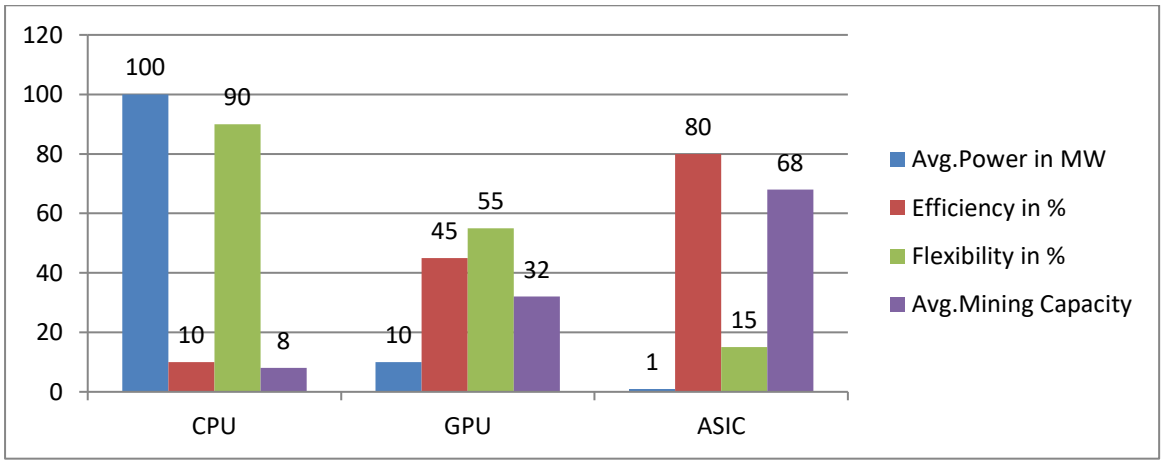

Figure 3. Parameterize analysis

VI. CONCLUSION

The blockchain technology offers a distributed ledger system that verifies transactions and ensures that once they are added to the chain, they cannot be altered in any way by unauthorised parties. In the event that someone does attempt to tamper with the data, it is simple to identify the deviation from the pattern and take preventative steps. Because the role of validating transactions is distributed among actors who have significant investment in the network, which can be measured as proof of stake or proof of investment, blockchain also eliminates the risks associated with a centralised architecture. This is accomplished through proof of investment or proof of stake. Internet users now have the power to generate value and verify the authenticity

of digital content thanks to a newly developed technology. It has the potential to transform a wide variety of commercial applications, including the sharing economy, data management, and prediction markets, among others. The findings of the survey that are reported in this article reveal that Blockchain technology offers a number of particular benefits for healthcare applications in comparison to other applications. Utilizing a lightweight distributed ledger system like IOTA is one way to further amplify the advantages offered by blockchain technology.

VII. REFERENCES

[1]. United States. Office of personnel management. A white paper: a fresh start for federal pay: the case for modernization. US Office of Personnel Management; 2002.

[2]. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2019. https://bitcoin.org/bitcoin.pdf.

[3]. Buterin V. A next-generation smart contract and decentralized application platform. White paper. January 2014.

[4]. Zhang P, White J, Schmidt DC, Lenz G. Applying software patterns to address interoperability in blockchain-based healthcare apps. June 5, 2017. arXiv preprint arXiv:1706.03700.

[5]. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. Adv. Comput. 2018;111:1e41.

[6]. Zhang P, White J, Schmidt D. Architectures and patterns for leveraging high-frequency, low-fidelity data in the healthcare domain. IEEE International Conference on Healthcare Informatics (ICHI). June 4, 2018. p. 463e4. IEEE.

[7]. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. Fhirchain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J January 1, 2018;16:267e78.

[8]. Epic. Epic community [Internet]. 2019 [cited 2018 Dec 18]. Available from, https://www.epic.com/.

[9]. Cerner. Ambulatory solutions j Cerner. Cerner e cerner.com [Internet]. 2019 [cited 2018 Dec 18]. Available from, https://www. cerner.com/.

[10]. McCoy AB, Wright A, Kahn MG, Shapiro JS, Bernstam EV, Sittig DF. Matching identifiers in electronic health records: implications for duplicate records and patient safety. BMJ Qual. Saf March 1, 2013;22(3):219e24.

[11]. Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. Ine-health networking, applications and services (Healthcom), 2017 IEEE 19th international conference on. October 12, 2017. p. 1e4. IEEE.

[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]. [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]. Liang X, Zhao J, Shetty S, Liu J, Li D. 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; October 2017. p. 1e5.

[25]. Esposito C, De Santis A, Tortora G, Chang H, Choo KKR. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing 2018;5(1): 31e7.

[26]. Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: a blockchain-based platform for healthcare information exchange. In: 2018 IEEE International conference on smart computing (SMARTCOMP). IEEE; June 2018. p. 49e56.

[27]. Theodouli A, Arakliotis S, Moschou K, Votis K, Tzovaras D. On the design of a blockchain-based system to facilitate healthcare data sharing. In: 2018 17th IEEE International Conference on trust, security and privacy in computing and Communications/ 12th IEEE International Conference on big data science and engineering (TrustCom/ BigDataSE). IEEE; August 2018. p. 1374e9.

[28]. Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. In: Proc. NIST workshop blockchain healthcare, vol. 1; 2016. p. 1e10.

[29]. Le Nguyen T. Blockchain in healthcare: a new technology benefit for both patients and doctors. In: 2018 Portland International Conference on management of engineering and technology (PICMET). IEEE; August 2018. p. 1e6.

[30]. Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, Guo Y, Wang FY. Blockchainpowered parallel healthcare systems based on the ACP approach. IEEE Transactions on Computational Social Systems 2018;(99):1e9.

[31]. Bhuiyan MZA, Zaman A, Wang T, Wang G, Tao H, Hassan MM. Blockchain and big data to transform the healthcare. In: Proceedings of the International Conference on data processing and applications. ACM; May 2018. p. 62e8.

[32]. Rathore H, Mohamed A, Al-Ali A, Du X, Guizani M. A review of security challenges, attacks and resolutions for wireless medical devices. In: Wireless communications and mobile computing Conference (IWCMC), 2017 13th International. IEEE; June 2017. p. 1495e501.

[33]. Fortune, U.S. Health care costs Skyrocketed to $3.65 trillion in 2018 [accessed on 14 Nov 2019]

[34]. Karafiloski E, Mishev A. Blockchain solutions for big data challenges: a literature review. In: IEEE EUROCON 2017 - 17th International Conference on smart technologies. IEEE; July 2017. p. 763e8.

[35]. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems 2018;42(7):130.

[36]. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017;5: 14757e67.

[37]. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems 2016;40(10):218.

[38]. NIS Cooperation Group, “EU coordinated risk assessment of the cybersecurity of 5G networks” .

[39]. Rathore H, Fu C, Mohamed A, Al-Ali A, Du X, Guizani M, Yu Z. Multi-layer security scheme for implantable medical devices. Neural Computing & Applications 2018: 1e14.

[40]. Rathore H, Al-Ali AK, Mohamed A, Du X, Guizani M. A novel deep learning strategy for classifying different attack patterns for deep brain implants. IEEE Access 2019;7: 24154e64.

[41]. Rathore H, Wenzel L, Al-Ali AK, Mohamed A, Du X, Guizani M. Multi-layer perceptron model on chip for secure diabetic treatment. IEEE Access 2018;6:44718e30.

[42]. Rathore H, Al-Ali A, Mohamed A, Du X, Guizani M. DTW based authentication for wireless medical device security. In: 2018 14th International Wireless communications & mobile computing Conference (IWCMC). IEEE; June 2018. p. 476e81.

[43]. Rathore H, Al-Ali A, Mohamed A, Du X, Guizani M. DLRT: deep learning approach for reliable diabetic treatment. In: GLOBECOM 2017 - 2017 IEEE Global communications Conference. IEEE; December 2017. p. 1e6.