Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)
IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2

Healthcare Domain in IoT with Blockchain Based Security- A Researcher's Perspectives

A.Yogeshwar Research Scholar,
Department of Computer Science,
Vels Institute of Science,Technology & Advanced Studies (VISTAS)
yogeshma@gmail.com

S. Kamalakkannan Associate Professor,
Department of Information Technology
Vels Institute of Science,Technology & Advanced Studies (VISTAS)
kannan.scs@velsuniv.ac.in

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICCS51141.2021.9432198

***Abstract*—The impact of Internet of Things (IoT) is most predominant and leading over the world. IoT is used to gather information/data from various sensors and other smart devices. The beneficiary of using technology of IoT can exchange information and enable to communicate with smart devices among themselves. In healthcare environment, IoT brings more convenient to doctors, nurses and patients. It can be more efficient for monitoring the illness patients and diagnosing very effective with reducing the cost. There are various security breaches and malignant attacks in healthcare system which are extremely vulnerable such as forgery, privacy leakage etc. Therefore these challenges and issues in security based on authentication and interoperability which bring to deteriorate. Recently, one of the key development in security is created by Blockchain (BC) technology which can exchange the data in secure manner. In many existing studies can be improved by enabling BC technology in the healthcare system. The main scope of BC technology has to convey effectively exchanging information between patient and other medical service parties based on some of the advantages such as authentication, immutability, decentralized storage, interoperability, distributed ledger, trustworthy and provides opportunity in a reliable manner and increase in productive. This paper presents challenges and problems for BC based IoT healthcare and provide with the security requirements of such domains due to traditional security measures. The aim of this paper is simply investigate how Blockchain will improve the healthcare environment within the IoT context. It also amalgamates the potential 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: Healthcare Domain, Blockchain, IoT, Security, Patient,. Electronic Health Records (EHR), Sensors

I. INTRODUCTION

IoT is considered as connecting a set of any network, anyplace, any service and anytime which is one of the integrated part of upcoming internet [1]. The main active player of IoT can be handled by interaction between various services, data providers, devices, sensors and applications allowed with smart communication technologies. It is not only connecting the related devices by employing the internet but also web-empowered exchange information to become smart based on empower systems with more abilities. The advancements in Wireless Sensors Networks (WSN) to Radio Frequency Identification (RFID) becomes risen as the result of IoT context which will detect and pass over internet by providing the abilities to activate [1]. Otherwise IoT can be defined by exchanging information with each other in virtual one in order to integrating the physical world[1][2]. This IoT link between smart devices provides a potentially advanced depiction of the actual reality, allowing for the creation of new fields of intelligent and brilliant applications in a variety of industries and projects.

In the pharmaceutical industry, advancement of healthcare system brought about greater competitiveness over the years and difficulties can overcome in this field. As a result, patient care can improve in healthcare environment where the users like nurses, doctors, physicians may able to work accordingly only by the better management of healthcare records. The entire process of patient care can be computed by providing an opportunity to assist managing and organizing the data which it is needed [3]. In the electronic healthcare system, stored historical data about the health of a patient can provide valuable information. Moreover, healthcare services of both urban and rural areas can be assembled and to study contagious. These data will be assisting to overcome the specific challenges and understanding the phenomena is the great values for researchers in several fields but the patient's data are treated as highly confidential information. The private information's of patients health records may have adverse effect which are unauthorized disclosure will damage the name of healthcare institution in the society. The essential thing is to protect the spreading of patient's health records so avoid embarrassing or unethical situations.

Healthcare domain in IoT has higher safety with better quality which has minimize the cost of services and reduced time based on the increased user experience with constant medical care[4][5][6]. The sensitivity of the data is the very essential parameter in Healthcare domain in IoT. Hence large quantity of information are generated which may consumes lot of power and obstructs the network. There are several challenges can occur in healthcare when the use of small sensors due to limiting the memory usage, limited power supply, limited network capacity and computer specifications [5] [7]. Hence several technologies are required to managed and integrated. In the healthcare required to generate a heterogeneous ecosystem by the use of multiple IoT technologies which are lowers its applicability and makes to complicate the framework. In general, IoT framework has interoperability issue particularly in healthcare domain [5][8][9]. The application of IoT in healthcare transforms it into more smart, fast and more accurate.

There is different IoT architecture in healthcare that brings start health care system are illustrated in figure.1.

FIGURE 1 Simple healthcare system architecture

Moreover, another essential issues are need to be considered by enhancing a healthcare IoT framework with the integration of heterogeneous model which are being to sustain trustworthiness of the data. In the data manipulation process, healthcare domain needs trustworthiness and security for prevention of laws and patient health record. Nowadays, information may turns out progressively predominant on mobile devices and cloud storage also sharing of record by a cause of availability at any time anywhere. The cloud data may cause rising the risk of malicious attack when the private information present on the shared storage [10]. In the shared network, blockchain can prevent the transfer of precarious data. The blockchain technology is the mechanism for solving serious data security, integrity and security challenges which is responsible for new potentials to store and distribute data in healthcare. Healthcare is one of the outstanding application in blockchain technology. The challenges based on blockchain in healthcare can overcome data privacy, storage, security and sharing [11,12].

Interoperability is the most essential needs in healthcare industry. The humans or machine are the two parties who can be able to exchange data or information accurately, securely, and continuously [13,14]. In the healthcare industry, the purpose of interoperability is to make it easier for healthcare providers and patients to share health-related information, such as Electronic Health Records (EHRs), so that data can be shared across the environment and deployed through multiple hospital systems [15,16]. Additionally, interoperability allows providers to access the medical records with secure manner and share the information between them by disregarding trust relationship and provider's location [17]. The healthcare data source is somewhat different which are considered for specifically more essential. Among the healthcare community, the factors of interoperability can be determined using blockchain technology is to manage, store and safely share EHR data [18]. The world economies, the tremendous pressure can be caused in healthcare infrastructures may rise of cost and software in the industry. Blockchain technology is improving healthcare outcomes for businesses and stakeholders in the healthcare industry by improving business performance, patient data management, improving patient outcomes, enhancing adherence, lowering costs, and allowing better use of healthcare-related data [19]. The potential of blockchain technology is also significant to impact the medical equipment and flow of drugs in a long and complex healthcare supply chain. The healthcare supply chain in blockchain technology has the potential to reduce the risk of illegal products putting patients at risk all over the world. In the Internet of Medical Things (IoMT), blockchain system is increasingly being tested in a variety of healthcare applications, including data management, storing, security and device connectivity.

A comprehensive analysis of basic security requirements of healthcare systems is one of the main contributions of this paper. In comparison to monotonic accessible state-of-the-art surveys, this paper offers an integrative research addressing security standards as well as challenges and open problems based on loopholes in current solutions, patients' information sharing and privacy promise concerning blockchain add-on in healthcare. It also filters out the exploding patterns in the region to include a baseline for several other researchers. It emphasizes that, in addition to other security solutions, blockchain might be able to get a scalable solution and decentralized to meet the increasing needs of the smart healthcare industry.

The remainder of the paper is organized as follows: Section 2 describes IoT based healthcare security requirements, Section 3 describes challenges using Blockchain in healthcare, Section 4 describes security solution based on Blockchain in smart healthcare systems, Section 5 describes integration of IoT healthcare and Blockchain, Section 6 ends with conclusion.

II. IOT BASED HEALTHCARE SECURITY REQUIREMENTS

In the medical field, the concept of IoT includes validation, knowledgeable and automated information compilation. Patients' personal information and discoveries are mostly addressed by IoT-enabled smart healthcare systems. If not protected with advanced

and powerful security measures, this data is highly vulnerable to malicious attacks. Furthermore, smart healthcare domains used some of the smart technologies and sensors which are limited in terms of resources with low processing and storage capabilities. As a result, they are unable to incorporate supporting security protocols [20] [21]. Additionally, such devices are mobile, they may require public network connections, including those found in hospitals, homes, and offices, adding to their vulnerability. The mechanism of designing dynamic and stable security is a difficult task with the exponential increase in connected IoT devices [22]. Several issues and challenges need to be addressed as any applications, services, and/or prototype in the domain. The healthcare-IoT research includes infrastructure, services, and applications, with requirements of interoperability, scalability and security, among others. Several guidelines and policies have been developed and enhanced for conveying IoT innovation in the medical field in numerous nations and associations. Furthermore, healthcare-IoT context forces developers, users and providers to interact with "strangers" entities and have to deal with various information from unknown sources. So, the healthcare-IoT domain may be a target of attackers. The vulnerability of communication between nodes makes security and authentication issues become a major factor through health IoT field. Several devices generating huge information in Health-IoT domain represent another challenge that creates another requirement for a common trust model to accommodate even the simplest of those devices. Enhancing the interoperability issue makes information understandable among all devices in the system. Zang et. al. [23] provided a new vision for trust by reconciling the two perspectives (interpersonal, organizational). They elaborated a theory on how the two types of trust work effectively together, where effective purchase intention relies on four boundary conditions. Also, they added regression analysis with fuzzy-set Qualitative Comparative Analysis (fsQCA). The heterogeneity of Electronic Health Records (EHRs) in health-IoT systems and complexity in accessing and reusing such data is seen as vital issues. Hence, this paper need comprehensive data models, supplemented with layer of semantic mechanisms between the healthcare systems. The interoperability of the semantic layer shall enable data reuse and achieve integrity, which relies on a unified structural/terminological framework that depends on a Basic Formal Ontology mechanism. This framework could have been more attractive if it had some reliability and authentication between its members. Several e-health systems can be developed by utilizing IoT devices. The authors in [24] proposed a model to monitor patients at risk, focusing on two elemental and critical aspects "prevention and effective intervention" to assist in medicinal emergency. The important security requirements in the IoT-enabled health care domain are outlined inTable1.

Table1.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 [21].
Integrity	Refers to the correctness of health data, either gathered or disseminated to the authorized entities without any fabrication or modification [25]. 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 [26].
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.
Authenticity	Refers to the truthfulness of the requesting entity, which means only the authentic party may access or modify the health data [27].
Non-repudiation	Ensures neither user nor patient can deny the provided data. It may be handled by digital signatures and encryption.
Access Control	Ensures controlled and legitimate access to the health data and information either public or private [27].
Privacy	Holds that the health data and information is available to authorized users only.
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 [28].
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.

Researchers have a great interest in studying the potential of IoT application on healthcare and medical systems. Several issues and challenges need to be addressed as any applications, services, and/or prototype in the domain. The healthcare-IoT research includes infrastructure, services, and applications, with requirements of interoperability, scalability and security, among others. Several guidelines and policies have been developed and enhanced for conveying IoT innovation in the medical field in numerous nations and associations. Furthermore, healthcare-IoT context forces developers, users and providers to interact with "strangers" entities and have to deal with various information from unknown sources. So, the healthcare-IoT domain may be a target of attackers [1] [7]. The vulnerability of communication between nodes makes security and authentication issues become a major

factor through health IoT field [4]. Several devices generating huge information in Health-IoT domain represent another challenge that creates another requirement for a common trust model to accommodate even the simplest of those devices. However, to ensure privacy and security of EHR when IoT is deployed without reducing the data usability, remains a critical challenge [8]. The utilizations for Internet of Things innovation was extended and changed. However, the system deficits guidelines for verification and approval of IoT edge devices and components. Security features will be required to shield IoT members and platforms from both data attacks and physical altering.

III. Challenges of Using the Blockchain in Healthcare

Even though Blockchain is a multidisciplinary concept with problems and constraints, it can be applied to a wide variety of areas. Researchers in this field are working to overcome or mitigate the negative effects of these factors. There are some of the issues and technical problems that Blockchain technology faces when used in healthcare [29].

1. **Throughput:** These may cause a network bottleneck due to rise of increased number of nodes and transactions by checking of more will be carried out in the network. The problems in healthcare domain has high throughput due to unless of fast access, the diagnosis may affect adversely to save the patient's life.
2. **Latency:** Validating a block takes a few minutes, which can be harmful to system security services because successful attacks will occur during that time. All the time, healthcare domain can be accessed dynamically which can affect adversely the analysis of examination due to the process of delay.
3. **Security:** If an entity gains control of 51 % of the network's computing capabilities, this can be adversely affected. This is a serious issue that needs to be addressed because a harmed healthcare system can lead to healthcare organizations losing their legitimacy.
4. **Resource consumption:** There are loss of resources involved due to spending lot of energy which can threatens the use of technology on the mining process. There are many devices are required to monitor patients in a medical environment due to high energy costs; furthermore, the use of blockchain will result in high processing and energy costs thus managing these costs is a challenge for businesses.
5. **Usability:** These systems are so complicated to handle due to usability is also a problem. Furthermore, users can need an Application Programming Interface (API) containing user-friendly features. Though health care providers may not have the IT professionals with same level of technical expertise. These systems should be very easy and more effective.
6. **Centralization:** Despite the fact that blockchain is a decentralized architecture which reduces network reliability and some approaches are known to standardize miners. Because this central nodes can be hacked and vulnerable in which malicious attacks can gain access to the data it stores.
7. **Privacy:** The Bitcoin framework has been widely accomplished by allowing blockchain to ensure the privacy of its nodes. The results of [30], on the other hand, contradict this assertion. Furthermore, approaches can provide this capability to blockchain-based systems are required [30]. The General Data Protection Regulation (GDPR) requires blockchain-based technologies to conform privacy laws and regulations.

IV. Blockchain-based Security Solutions in Smart Healthcare Systems

In healthcare services, there are various cyber-attacks involved in past decade. However, the existing techniques are not considered with security over data storage and transmissions that became an essential factor in providing privacy and protecting patient's health data in healthcare. Hence, this study presented the implementation model for securing the information's of smart healthcare which is the major issues faced in the current healthcare like protecting patient's records available in the healthcare organization, breaching of patients sensitive health records for stake may cause ineffective delivery of data towards patient's healthcare. One of the scenarios faced due to unsecured record is delay in processing of patients records from one service provider to other service provider. Thus, the EHR has facing such limitation practice that can be overcome by latest technology as Blockchain which is recently adopted in various governments, public-private partnered projects and private projects [31]. Table 2 has summaries certain security solution using Blockchain in smart healthcare organization with its advantages.

TABLE 2 Security solution using Blockchain in smart healthcare organization

Author	Problem description	Advantage	Security solution by Blockchain
Dagher et.al[32]	Access control, data obfuscation	Data ownership, integrity, and scalability	Instead of simulating monetary-based mining, arrangement of smart with ethereum-based and cryptography.
Xu et.al[33]	Failure in single point, Sybil	Privacy, accountability, and	Encrypting data, control access, key

	attack and privacy leakage.	on-demand rescission	management and privacy preservation.
Omar et.al[34]	Privacy, eavesdrop, and intrusion attacks	Pseudonymity, privacy, integrity, accountability	Distributed web platform, access control
Zhang and Lin [35]	Privacy issues	Control access, privacy preserving, secured search, auditing, and rescission in time control	Private blockchain and consortium blockchain
Griggs et.al[36]	Real-time patient monitoring security	Immutability, confidentiality, availability, privacy, transparency and traceability.	Permissioned and consortium-managed blockchain
Chen et.al [37]	Data leakage, malicious operation, and dishonest user	The outcome of reliable search, analysis of fairness, integrity, confidentiality, traceability and anti-tampering	Customized search index-based Blockchain
Kleinaki et.al[38]	Problem in repudiation and data integrity.	Non-repudiation, data quality discrimination and data integrity	Blockchain-based notarization
Abdellatif et.al[39]	Issues in scalability, Sharing of data, and Quality of Service (QoS)	Efficient and remote monitoring in scalability, sharing of data and QoS.	Smart and Secured Healthcare (SSH) system using Blockchain
Du et.al[40]	Issue in sharing of anonymous data and privacy.	Effective in handling of transaction, tamper-resistance, higher fault tolerance and privacy protection	Blockchain arrangement with two-layer consortium blockchain and with recent arrangement of MBFT algorithm
Ali et.al[41]	Failure in single point, DoS, and certain attacks like data sniffing, man in the middle, etc.	Efficient with delivering message in time, identity management, privacy preservation, immutability and security.	Public blockchain with RHM based solution

In both identity and access control, the information can authenticates is a major challenge. A username, password, and thumbprint may be used to verify a person's identity. Otherwise, private keys are used for authentication of an identity to sign every transaction based on blockchain technology. Another main challenges is user preferences which can covers by data auditing trail and accord of their data usage. An entire log of electronic data changing, removing and creating the data auditing trail can be supported and maintained by blockchain. In the smart healthcare domain, authorization is one of the major challenges to accomplish action using various stakeholders. For each and every stakeholders, policy will be assigned with right access to data. Moreover, accessing the patient data do not have the self-ownership. Hence blockchain technology being very thankful which maintain the legitimate access to data, authorization and data to access the self-ownership of the patients. The most essential role in the blockchain technology is efficiency which is faced in the healthcare domain. The results of cost and time overheads based on delivery of services, logistics, and administration on inefficiency can attained minimum advantages [42]. In policy making, reasons could be flaws and exchange of data to be inefficient. Moreover, EHR should be ensured by logging and monitoring to sensitive healthcare data of every access to prevent non-monitoring access. The most of the healthcare organization could not achieve this difficulties also does not follow the process of severe access of authorization. Additionally, good security needs are not available based on the infrastructure of patients' databases. Blockchain may be a solution to these problems, leading to the resolution of a larger issue of authentication and privacy. It also promotes time-stamping and data auditing, which could aid patients in identifying changes in data over time and also the identification of the individual who can addressed the problem. Patients can grant third parties access to their data in a blockchain environment, but they cannot store it. To summarize, blockchain-based technologies outperform current conventional structures.

V. IOT-HEALTHCARE AND BLOCKCHAIN INTEGRATION

Blockchain technology in the healthcare context plays a key role in achieving security, trust and authentication between all members (doctors, hospital, patients and other medical parts) in healthcare domain. Mettler et al. [43] described examples showing the importance of Blockchain can be used in the healthcare industry in a variety of ways. BC improves medication protection while lowering health-care follow-up costs. The benefits of Blockchain for healthcare applications have been identified, and it will have a significant impact on the power balance between established market participants in healthcare. A prototype of Blockchain technology that enhance and guarantees privacy, security, and accessibility for overseeing and sharing EMR information for malignant growth (cancer) patient care is proposed in [44]. In

addition, BC accomplished fine-grained EMR information for authority and lessen the expense. Expanding the structure of a medical record and its metadata, as well as using the semantics of health records, will make this structure more accurate. The ability to construct a privacy-preserving predictive model on healthcare data in a robust and safe manner is a crucial goal to achieve [45]. Authors integrate online machine learning with Blockchains by constructing a system (Model Chain) to reach high level of confidentiality and accomplish privacy-protection. Research can be done without uncovering any patient sensitive health data. Moreover, they structure algorithms for evidence-based decision making working in real-time systems and online which needs higher interoperability between different infrastructures. Healthcare industry is totally based on data that are gathered from patient or any person through health system. These healthcare data usually arises some concerns over data confidentiality and privacy [46]. To begin with, they only proposed storing and exchanging EMRs which ignoring the valuable and abundant Personal Healthcare Data (PHD). The criteria for managing and retrieving large amounts of PHD differ greatly from those for storing and sharing EMRs which gets posing new challenges in terms of device based on throughput and accuracy. Second, current systems store EHRs in the cloud, with advanced access management methodologies in place to avoid the spread of unwanted information [47]. However, this framework vigorously depends on the security of the cloud space. Others looked at more sophisticated programs to recognize foresight in healthcare data analysis and develop the test to obtain precision medicine [48]. The authors provided an inclusive roadmap guide on how to implement such systems. Their framework or application should be implemented and experimented to assess their qualities and shortcomings.

TABLE.3 IOT Technique comparison for healthcare in the blockchain technology

Author	Blockchain technology	Types of data	Merits	Demerits
Griggs et.al[36]	Public blockchain with proof of concept in ethereum platform.	Sensors data	WBAN Integration by smart arrangement to monitor patient securely with automation.	Data absorption is not efficient
Rahman et.al[49]	Private blockchain with hyperledger and ethereum platform.	IoT-Multimedia data	Mobile medical experts assist in securely sharing of dyslexia diagnosis data.	Time consumption is more during upload
Jo et.al[50]	Proof of work with ethereum platform.	Sensors data	The arrangement of PoW mechanism has improved transparency, data storage and data security.	Risk in security over real-time monitoring due to rapid block time
Ichikawa et.al[51]	Hyperledger and fabric platform	EHR and sensors data	Secured with network fault like node down distribution.	Vulnerable to attack
Azaria et.al[53] (2016)	MedRec	Sharing health information	Improve data quality for medical researches	Not have contract encryption
Uddin et.al[54] (2018)	Patient centric agent (PCA)	Remote care with IoT	Provide access control role-based	Requires devices with high power processing for encryption
Sandgaard and Wishstar [55] (2018)	MediChain	Sharing health information	Reduces risk to identify the patient from data leaked	Problems with privacy
Albeyatti [56] (2018)	Medicalchain	Sharing health information	Patient control access with MedTokens	There are risks for acquiring the MedTokens
Saia [57] (2018)	Public blockchain	Sensor data	Ensuring anonymity and immutability, Log activity of entity and object.	Computational overhead is high
Kuo et.al[58] (2018)	Proof-of-information	Medical records	Enhanced privacy in medical health prediction model.	Vulnerable to attack
Wang et.al[59] (2018)	Proof of stake. Private blockchain	Medical records	Artificial healthcare systems	Limited treatment scenarios are included.

While Blockchain adds value to EHRs which are still faces challenges that lead to the field's drawbacks. However, rather than technological barriers, educational barriers stand in the way of using Blockchain in this area. Furthermore, several privacy laws that exist for IoT-enabled health records [52]. The proper encryption of patients' data are combined with an effective control policy will help a lot in this domain with trust management. Due to the growing scale of produced data over time, scalability issues are also exist. By implementing Blockchain, every node in the network would have access to a patient's entire medical record which are potentially caused by bandwidth and data storage issues.

VI. CONCLUSION

Health-IoT environment are significant and essential to set up and constitute the necessary security, protection and privacy techniques to avoid any type of security break and vulnerability. The healthcare organization with IoT is likely to be crucial in security challenges and threats. In order to avoid those challenges and treats, it is essential for understanding the security need in healthcare systems. The conventional mechanism of security didn't provide all kind of security needed to IoT-enabled healthcare system because of low scalability, failure in single point, high cost and resource constrained in nature for the IoT devices. This study has focused on addressing the need of security in IoT enabled healthcare system with blockchain based application security solutions. Moreover, the solutions of blockchain to overcome various security problems are discussed in a scalable, distributive and an efficient manner. There are various healthcare providers are facing specific road blocks because of an ownership and access control factors which may prohibit for adopting blockchain. Hence, the psychological challenges have been encountered by an organization of healthcare that need to be considered and deal with addressing various privacy, trust, integrity and security. In short, this study aimed to present a number of works for researchers interested in implementing Blockchain-based healthcare systems. Also this paper discussed some of the platforms for building Blockchain-based healthcare applications, presenting their limitations and advantages. Table 3 sets out the pros and cons of these methods to form a point of comparison between these methods. As a result, we concluded that a line of research is the sharing of healthcare information and the use of Hyperledger Fabric platform which are Robust against network fault such as distributed node down. In addition, still the challenges of block chain 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] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, "On Blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems., Vol-88, pg-173-190, 2018.

[2] D. Singh, G. Tripathi and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in 2014 IEEE world forum on Internet of Things (WF-IoT)., 2014.

[3] Liam Bell, William J. Buchanan, Jonathan Cameron, and Owen Lo, "Applications of blockchain within healthcare.Blockchain in Healthcare Today",vol-1, 2018, pp-1–7. DOI:https://doi.org/10.30953/bhty.v1.8

[4] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," IEEE Access., vol-3, pp-678-708, 2015.

[5] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi and L. Tarricone, "An IoT-aware architecture for smart healthcare systems," IEEE Internet of Things Journal, vol-2, pp-515-526, 2015.

[6] P. P. Ray, D. Dash and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," Journal of Network and Computer Applications., vol-140, pp-1-22, 2019.

[7] T. McGhin, K.-K. R. Choo, C. Z. Liu and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," Journal of Network and Computer Applications, 2019.

[8] J.-J. Yang, J.-Q. Li and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems., vol-43, pp-74-86 ,2015.

[9] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja and K. Wasielewska, "Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective," Journal of Network and Computer Applications., vol-81, pp-111-124, 2017.

[10] Y. Yang, X. Zheng and C. Tang, "Lightweight distributed secure data management system for health internet of things,"Journal of Network and Computer Applications., vol-89, pp-26-37, 2017.

[11] Rawal, V.; Mascarenhas, P.; Shah, M.; Kondaka, S.S, "White Paper: Blockchain for Healthcare an Opportunity to Address Many Complex Challenges in Healthcare", CitiusTech: Princeton, NJ, USA, 2017.

[12] Engelhardt, M.A, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector", Technol. Innov. Manag. Rev. vol-7, pp-22–34, 2017.

[13] Al Ridhawi, I.; Aloqaily, M.; Kotb, Y.; Al Ridhawi, Y.; Jararweh, Y, "A collaborative mobile edge computing and user solution for service composition in 5G systems", Trans. Emerg. Telecommun. Technol. vol-29, e3446, 2018.

[14] Al Ridhawi, I.; Aloqaily, M.; Kantarci, B.; Jararweh, Y.; Mouftah, H.T, "A continuous diversified vehicular cloud service availability framework for smart cities", Comput. Netw, vol-145, pp-207–218, 2018.

[15] Gordon, W.J.; Catalini, C, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", Comput. Struct. Biotechnol. J. vol-16, pp-224–230, 2018.

[16] Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile, "Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustain. Cities Soc, vol-39, pp-283–297, 2018.

[17] Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G, "Blockchain technology use cases in healthcare", In Advances in Computers; Elsevier: Amsterdam, The Netherlands, Vol-111, pp. 1–41, 2018.

[18] Casino, F.; Dasaklis, T.K.; Patsakis, C, "A systematic literature review of blockchain-based applications: Current status, classification and open issues" Telemat. Inform, vol-36, 5pp-5–81, 2019.

[19] Mackey, T.K.; Kuo, T.T.; Gummadi, B.; Clauson, K.A.; Church, G.; Grishin, D.; Obbad, K.; Barkovich, R.;Palombini, M, 'Fit-for-purpose?'—Challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. vol-17,pp- 68, 2019.

[20] 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, vol- 134, pp-198–206, 2019.

[21] 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, vol-8 issuse-1, 2019.

[22] 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 vol-19, issues- 8, 2019, pp-1788.

[23] S. Zheng, S. F. Hui and Z. Yang, "Hospital trust or doctor trust? A fuzzy analysis of trust in the health care setting," Journal of Business Research., Vol-78,pp- 217-225, 2017.

[24] I. Chiuchisan, I. Chiuchisan and M. Dimian, "Internet of Things for e-Health: An approach to medical applications," in 2015 International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)., 2015.

[25] 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, vol-99, issues-8, pp-1966–1973, 2016.

[26] 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.

[27] 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, vol-96, pp-410–424, 2019.

[28] 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, vol- 9,issues- 5, 2020, pp-716.

[29] ERIKSON JÚLIO DE AGUIAR and BRUNO S, "A Survey of Blockchain-Based Strategies for Healthcare", ACM Computing Surveys, Vol. 53, No. 2, Article 27, 2020.

[30] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang, "Blockchain challenges and opportunities: A survey", International Journal of Web and Grid Services,vol-14, issues-4, 2018, pp-352–375.

[31] N. Kshetri, Blockchain and electronic healthcare records [cybertrust], Computer vol-51, issues-12 ,2018, pp-59–63.

[32] 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, vol- 39 ,2018, pp-283–297.

[33] 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, vol- 6, issues-5,2019,pp-8770–8781.

[34] 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.

[35] A. Zhang, X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain", Journal of medical systems, vol- 42, issues-8,2018, pp-140.

[36] 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, vol- 42, issues-7, 2018, pp-130.

[37] 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,vol- 95, 2019, pp-420–429.

[38] 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, vol- 16, 2018,pp-288–297.

[39] 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.

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

[41] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere, F. Antonelli, "A decentralized peer-to-peer remote health monitoring system", Sensors, vol-20, issues-6,2020,pp-1656.

[42] 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, vol- 19, issues-14, 2019,pp-3119.

[43] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.

[44] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher and F. Wang, "Secure and trustable electronic medical records sharing using Blockchain," in AMIA Annual Symposium Proceedings., 2017.

[45] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private Blockchain networks," arXiv preprint arXiv: 1802.01746., 2018.

[46] Z. Shae and J. J. P. Tsai, "On the design of a Blockchain platform for clinical trial and precision medicine," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017.

[47] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on Blockchain environment," Future Generation Computer Systems., vol-95,pp- 511-521,2019.

[48] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak and others, "Converging Blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," Oncotarget.,vol-9, pp-5665,2018.

[49]Rahman, M.A.; Hassanain, E.; Rashid, M.M.; Barnes, S.J.; Hossain, M.S, "Spatial Blockchain-Based Secure Mass Screening Framework for Children With Dyslexia",IEEE Access , vol-6, pp-61876–61885,2018.

[50] Jo, B.; Khan, R.; Lee, Y.S, "Hybrid Blockchain and Internet-of-Things Network for Underground Structure Health Monitoring", Sensors , vol-18, pp-4268,2018.

[51] Ichikawa, D.; Kashiyama, M.; Ueno, T, "Tamper-resistant mobile health using blockchain technology".JMIR mHealth uHealth, vol-5, pp--111, 2017.

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

[53] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman, "MedRec: Using blockchain for medical data access and permission management", In 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp-25-30.DOI:https://doi.org/10.1109/OBD.2016.11

[54] Md. Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture", IEEE Access 6, 2018, pp-32700-32726. DOI:https://doi.org/10.
1109/ACCESS.2018.2846779

[55] Joachim Sandgaard and Steve Wishstar. 2018. MedChain. Retrieved September 30, 2018 from http://medchain.us/doc/Medchain%20Whitepaper%20v1.0.pdf [White Paper].

[56] Abdullah Albeyatti. 2018. Meddicalchain. Retrieved September 30, 2018 from https://medicalchain.com/ Medicalchain-Whitepaper-EN.pdf [White paper].

[57] Saia, R, "Internet of Entities (IoE): A Blockchain-based Distributed Paradigm to Security",arXiv 2018, arXiv:1808.08809.

[58] Kuo, T.T.; Ohno-Machado, L, "ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks", arXiv 2018, arXiv:1802.01746.

[59] Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang F.Y, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach", IEEE Trans. Comput. Soc. Syst. 2018, Vol-5, pp-942–950.