

Blockchain Technology and IoT-healthcare: State-of-the-Arts, Challenges and Trends

Eman M. Abou Nassar^{1,*} and Passent Elkafrawy^{1,2}

¹Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom, Menoufia, Egypt.

²Nile University, School of Information Technology and Computer Science, 6 October, Giza, Egypt.

Received: 2 Sep. 2019, Revised: 5 Oct. 2019, Accepted: 21 Oct. 2019.

Published online: 1 Nov. 2020.

Abstract: In recent years, the Internet of Things known as IoT are widely used and their impact is prevalent and dominant. Variety of IoT known as smart devices and sensors use the internet to gather data. IoT morphs the traditional sensing devices to become selective, autonomous and independent. The advances in technology enable smart devices to communicate and exchange information among themselves. The application of IoT in healthcare environment brings great comfortable to patients, doctors and care providers. Illness's monitoring and diagnosis are more effective, efficient and cost reduction. However, they have suffer from challenges in the security (trustworthy and data reliability), authentication and interoperability.

Blockchain technology creates as a key development in security that changes the way by which we share information. The Blockchain can be applied into healthcare enabling our existing frameworks to be improved. Blockchain technology has a scope of advantages, such as decentralized storage, distributed ledger, interoperability, authentication, trustworthy, immutability and offer the opportunity to convey secure and exceptionally effective exchange transaction between patient, supplier and other medicinal services parties in a progressively productive and consistent manner. The benefits of Blockchain technology enable health-IoT system that is integrated, seamless and more confidential and with an increased level of cooperation or compliance. This paper centers around activities and presents challenges in Blockchain application in the IoT-healthcare domain and analyze the most significant contribution. It will simply investigate how Blockchain will improve the healthcare environment within the IoT context.

Keywords: Blockchain, Healthcare environment, IoT-context, interoperability, trustworthy, Vulnerabilities, Survey.

1 Introduction

The Internet of Things (IoT) is an integrated part of the Future Internet, which is considered as a concept reflected as a "connected set of anything, anyone, anyplace, anytime, any service, and any network"[1]. IoT is the main active player that allowed smart communication technologies and handled the interactions between several devices, sensors, services, applications, and data providers. The IoT environment is not just connecting associated devices by utilizing the Internet; however, it is a web-empowered information exchange so as to empower systems with more abilities to become smart. IoT-context has risen as a result of advancements in Wireless Sensors Networks (WSN) to Radio Frequency Identification (RFID); which furnish the abilities to activate with, detect and pass on over the Internet [1]. In other words, IoT aims to integrate the physical world with the virtual one, where things can exchange information and communicate with each other [1] [2]. This association between smart devices through IoT makes conceivably an advanced portrayal of this present reality, through which shifted fields of intelligent and brilliant applications in a lot of industries and ventures can be developed. Applications in the medical domain, smart cities, waste management, traffic congestion, security, emergency services, 4G industry, healthcare and transportation can benefit from such advancement [3][4]. Healthcare and biomedical domains are considered one of the most appealing applications for the IoT-environment. Enhancing healthcare services and developing smart biomedical systems is one of the most inspiring objectives in the coming era [1] [3] [5].

Healthcare systems can be enhanced by connecting devices, such as various tiny sensors, to construct an IoT network devoted to healthcare assessment. Such network can allow for remote health monitoring and automatic critical cases detection, for elderly care, fitness programs and chronic diseases (heart failure, respiratory diseases, hypertension or diabetes) [6]. IoT healthcare systems shall decrease *time* and *cost* of services, increase *safety* and *quality* of healthcare, with a continuous medical care and higher user's experience [5] [7] [8]. IoT-healthcare applications have very important characteristics due the sensitivity of the data, information is generated in huge volume which congests the network and consumes great processing power. As a matter of fact, the use of the tiny sensors in health care impose a number of challenges due to restrictions in network capacity, computer specifications, memory limits and restricted power supply [1] [7] [9]. For which various technologies need to be integrated and managed. The use of multiple IoT technologies, as required in healthcare, generates a heterogeneous ecosystem that complicates the system and lowers its applicability. The interoperability issue becomes a significant area in IoT systems in general and in medical systems in particular [7] [10] [11] [12].

In addition to the present challenge of developing an integrated heterogeneous health-IoT system, being able to maintain trustworthy of the data is another significant concern to be considered. The Healthcare industry requires security and trustworthy in the data manipulation process due to patients' medical data confidentiality and protection legislations. Recent days, sharing of records and information turns out to be increasingly predominant on cloud storage and mobile devices due to its availability anywhere anytime. Although, data on the cloud increases the danger of malicious attacks and the disclosure of private data on shared storage [9] [13]. Blockchain for that is used to protect the exchange of critical data on a shared network.

In this paper, we will discuss the advantage of integrating Blockchain technology into IoT-healthcare systems. Featuring Blockchain capability and addressing the difficulties involved in its applicability. The main contributions can be summarized as: first, a survey on the state-of-the-art methods of achieving interoperability on IoT-based networks with specific emphasis on oncology mechanisms. Second, investigating the various methods of incorporating health-IoT environment and Blockchain technology. Third, reviewing the potential advantages, difficulties, and open issues of the integration of Blockchain in IoT-medical services. Forth, listing existing IoT-medical services based Blockchain stages and applications.

For the rest of the paper is organized as follows: Section II presents related issues and problems facing healthcare. Section III introduces Blockchain and ontology technologies and their methods and applications that can be directed to solve the healthcare challenges. Section IV presents state of the art Blockchain platforms for IoT-healthcare and Blockchain applications. Finally, a conclusions and future work are introduced in Section V.

2 IOT-Healthcare Environments

In the coming era, IoT will be highly adopted in healthcare whereas new Health-IoT applications and devices will be pervasively common in the market. Healthcare applications and devices are relied upon to manage essential private data, as electronic patient records (EPR) and hospital patient records (HPR). A Healthcare system is actually an important trend adopted to acquire evidence based medical care for patients and medical service provider. In addition, to ensure integrity, quality, value, and safety in health care domain [5] [14]. Health-IoT is a collection of various medical devices, tiny sensors, and investigative devices (imaging devices), considered as smart objects building up the IoT-medical ecosystem. IoT technology enables and is responsible for generating several healthcare services in order to provide a set of healthcare solutions. However, a standard definition of IoT services in healthcare context still does not exist, whereas certain services are not distinguished in particular solutions or applications. As a result, the problem of *heterogeneity* has emerged as a crucial factor in health-IoT environments.

Health-IoT includes numerous medical monitoring devices as remote physiological information monitoring, chronic diseases diagnosis, rehabilitation training, and elderly care [13] [15]. The patients' data gathered from sensors and monitoring devices can be read through an internet browser on a normal PC and through Applications on mobiles and hand held devices.

Medical staff can use these devices to monitor patients' health-state and/or send to patients' information about their own treatment or medication. Patients may collaborate with medicinal staff and other patients for long range interpersonal communication and activities for prognosis and effective monitoring their treatment [5]. Therefore, all these data management tools must be safe and secure. Accordingly, in healthcare *trustable* systems are required for reliable decision support systems that can assist doctors, hospitals, patients and research in the medical field [7] [16] [17] [18] [9]. Accordingly, an interoperable trust model based is required using ontology mechanism and trust matching algorithm to treat two problems interoperability and trust issues, which will be explained in section IV.

2.1 Interoperability

Interoperability is characterized as the capacity of at least two implementations of systems or parts from various producers to share, reuse, exchange information and exchange information from each other by “relying on each other’s services as specified by a common standard” [11] [12] [19] [20]. Black stock et al.[21] , in 2014, achieved integrity-based web services through IoT hubs to assemble data utilized by web protocols. They introduced “IoT hubs” to gather things. Other, studies reused existing knowledge-based representations to annotate metadata and stream data collected from sensors to elevate system interoperability [14] [22] [23]. In [24], the perception of “Semantic Gateway as Service” (SGS) has been suggested as a channel between IoT points of service for interoperability. Communication is accomplished by standardizing data using SSN ontology and multi-protocol proxy for data exchange. In [25] the authors addressed challenges of a complete common layer for a data model with semantic interoperability mechanisms. The main restriction stopping interoperability is the actual deployment of medical data storage as a centralized repository. Isolated centralized data storage nodes (Islands) generates several issues. One of which is fragmentation of health data, as data cannot be shared. Data is heterogeneous thus accessibility is difficult, lacking interoperability in medical data. Another issue is that data accessibility becomes slow, the lack of data quality, patient agency, and quantity for medical research [14] [20]. New data are generated daily and stored in variety of hospitals [26]. These records that are dispersed in different hospitals can be lost and difficult to be accessed by patients [20] [27]. Also, these records can end up fragmented because of centralized nature of health system [27] . Finally, centralized information authorities are needed to ensure a confident and reliable database in an untrusted network.

2.2 Security

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] [9].

The vulnerability of communication between nodes makes security and authentication issues become a major factor through health IoT field [5] [28] . 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. [29] 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, we need comprehensive data models, supplemented with layer of semantic mechanisms [30] 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 [15] proposed a model to monitor patients at risk, focusing on two elemental and critical aspects “prevention and effective intervention” to assist in medicinal emergency. However, to ensure privacy and security of

EHR when IoT is deployed without reducing the data usability, remains a critical challenge[10] . Bernabe et al. [31] presented adaptable trust-mindful access control framework to supply “end to end” and “solid security”, relied on a trust model and authorized techniques.

Yang et al [13] created LDAC-KS system for the resource limited devices on IoT-health environment with efficient keyword search function. LDAC-KS secured the data and accomplished distributed access control and productive information recovery on ensured EHR records. 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.

3 Blockchain Technology

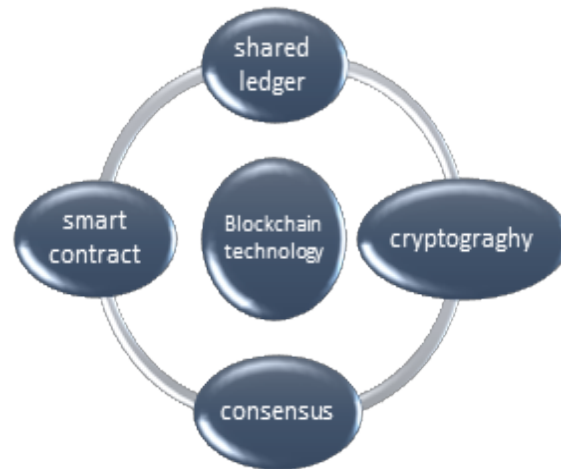


Fig. 1: Block chain Technology Component.

The Blockchain Technology serves as a decentralized method to manage IoT framework tackling a large number of the issues above. In an IoT framework, the Blockchain can keep an unchanging or immutable record of the historical knowledge of intelligent devices. This element empowers the independence (autonomous) of smart devices without the requirement for a centralized authority. Therefore, Blockchain opens the portal to a movement of IoT circumstances that were strikingly troublesome, or even difficult to actualize without [32] [33]. Also, one of the most invigorating limits of Blockchain is the ability to keep up a decentralized, believed record of all transactions occurring in a framework. This capacity is major to enable the various compliances and regulatory essentials of Industrial IoT (IIoT) applications without the need to rely upon a centralized model. Embracing an institutionalized shared correspondence (peer-to-peer) model to process several billions of transactions between devices will essentially diminish the expenses related with installing, preserving and keeping up huge concentrated data centers. Moreover, this will disseminate calculation and storage needs over the billions of devices that structure IoT networks [1] [9]. Our daily decisions in our real world are taken based on relational calculation and trust with another entity to take trustworthy decision. Hence, the IoT-system that improved the interoperability need to be more secured and with confidentiality and trustworthy between its members. The decentralized, independent, and trustless capacities of the Blockchain make it an ideal section to transform into an essential segment of IoT-context. Blockchain is essentially a decentralized, appropriated, shared, and immutable database record that stores library of benefits and exchanges over a distributed Peer to Peer (P2P) arrangement providing a global dispersed trust.

Blockchain systems are Distributed Ledgers Technology (DLT) with a mechanism to allow transactions to be verified by a group of (consensus) unreliable actors called miners [1] [34]. It gives distributed, transparent, immutable, reliable and auditable records. The Blockchain can be counseled transparently and completely, enabling access to all data exchanges or transactions that have happened since the main transaction of the system. The miners are members liable for generating the proof of work (PoW) or mining. The idea of verification of work is one of the keys to empower trustless agreement in Blockchain. The confirmation of work comprises of a computationally escalated task that is fundamental for the generation of blocks over the chain. It is intricate to understand and simultaneously effectively unquestionable once finished [1] [9]. When a miner finishes the proof of work, it distributes the new block over the network and the remainder of this network checks its legitimacy before adding it to the chain. Beside trustless consensus, cryptography and shared ledger Blockchain present another technology called smart contract (SC) as shown in figure 1. The SC is a computer program or protocol that allow a contract to be automatically executed or enforced considering a set of predefined conditions.

Blockchain can be a key empowering innovation for giving feasible security answers for now testing IoT security issues [16] [17] [35] [36]. In addition, the frameworks cooperate with one another, it's basic to have a concurrent interoperability standard, which is protected and valid. Without a strong bottom-top structure we will exert higher risks and attacks with each device added to the IoT-environment. What we need is a safe and reliable IoT network with security ensured and high level of trust and privacy preserved without being isolated within the same ecosystem. That is an extreme exchange off yet not feasible and Blockchain innovation is an appealing alternative to achieve these needs [3] [11] [23].

4 IOT-Healthcare and Blockchain Integration

Blockchain engineering has a plenty of features that can be used in the healthcare environment as shown in figure 2.

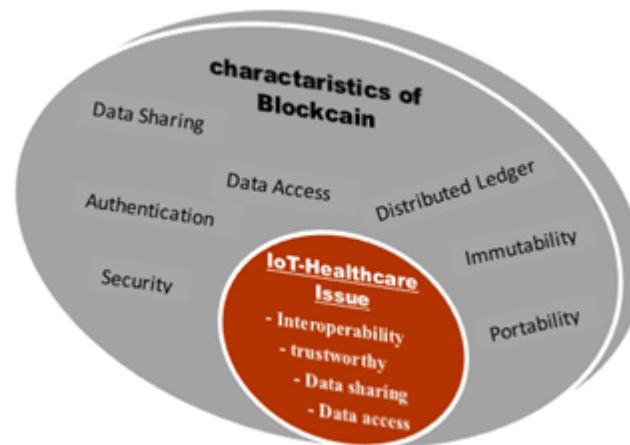


Fig.2: Blockchain characteristics.

These preferences are characteristic to the framework based Blockchain innovation and can be applied to a wide zone of frameworks and ventures. The highlights to be presented explicitly in this part are trustworthy, confirmation, integration and decentralized stockpiling.

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 and et al. [17] described examples showing the importance of Blockchain and how it offers numerous opportunities for usage in the healthcare sector. BC increases that safety in relation to drugs, and health-related follow-up costs are reduced. Identified benefits of Blockchain compared to conventional distributed databases for biomedical/ health care applications, and will strongly affect the balance of power between existing market players in healthcare [18].

A prototype of Blockchain technology that enhance and guarantees privacy, security, and accessibility for overseeing and sharing Electronic medicinal records (EMR) information for malignant growth (cancer) patient care is proposed in [37]. In addition, BC accomplished fine-grained EMR information for authority and lessen the expense. This structure can be increasingly effective by expanding the structure of a patient record and its metadata, utilizing the semantics of health information. The capability to robustly and securely construct privacy-preserving predictive model on healthcare data is an essential goal to be achieve [38]. 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. As authors in [39] [40].

suffer from two problems. First, they have considered storing and sharing only electronic medical records (EMRs) and ignored the beneficial and plentiful personal healthcare data (PHD). The requirements of storing and sharing the large amount of PHD is. considered more significantly from storing and sharing the EMRs, which gets new challenges in the aspect of system throughput and righteousness. Second, the existing systems store the EHRs in the cloud environment with sophisticated access control methodology to prevent undesired information dissemination [41]. However, this framework vigorously depends on the security of the cloud space. Others studied more advanced systems to acknowledge prescient investigation of healthcare information and advance the examination to achieve precision medicine [42]. 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.

Several of the proposed frameworks, systems, models and architectures, such as [42], need to be implemented and tested to Evaluate their qualities and shortcomings. Besides, for completely received Blockchain in operational healthcare conditions

The interoperability open-principles should be characterized to ensure communication between diverse Blockchain products. It is hence significant that analysts start investigating the trustworthy and interoperability issues and the institutionalization forms. The challenges of data security and authentication, interoperability, integrity and speed that depict Blockchain-based healthcare applications are largely open research. Such research requires purposeful commitment so as to improve partners' trust in the utilization of the innovation and to advance its reception in medicinal services.

5 Conclusions and Future Work

The IoT-healthcare environment based Blockchain innovation application is as yet a rising field, there is a requirement from scientists to grow more models, frameworks and proof-of-concepts to go profoundly into the comprehension and acknowledgment of the innovation in connection to its application.

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. We shall have the option to increase security and protection in e-Health. So as to have proficient e-Health arrangement, it is significant we join a portion of the recommended solutions proposed in any system or model for e-Health. Blockchain engineering considers a key challenge that address a lot of restriction faced by healthcare field. Such as healthcare wearable devices and patient sensitive health record need to be more secure with high level of authentications, trust and privacy preserving. Blockchain Authentication based Trust Models covered all these issues and shows how to use immutability of the Blockchain technology to provide solutions to high problems in the field of decentralized health-IoT networks. Our future goal is to develop a fully-fledged healthcare data sharing and identity sharing platform. Furthermore, research needs to be focused on the domain of identity verification, through the emergency state reinforcement plans or emergency protocols can be utilized to permit a specialist mentor to access the records without confirmation. Moreover, we need to implement and achieve a form of privacy-protection strategy called differential privacy to ensure high level of trustworthy between health-IoT members.

In this study, a finite volume solution of unsteady incompressible Navier-Stokes equations emphasizing 2D channel flow is presented. Central difference and backward difference are used to approximate the derivatives at the faces of the control volumes. A MATLAB code is developed to implement the finite volume discretization. The velocity and pressure are computed using the MATLAB code and the results obtained are compared with that of the accepted CFD commercial code, ANSYS Fluent. The MATLAB code and ANSYS Fluent results are nearly identical which indicate that the governing equations are discretized properly, the boundary conditions are implemented precisely and the code is written correctly. Backward difference approximation of derivatives creates a conducive environment to employ the boundary conditions of the flow in the finite volume discretization. Alternative way is provided to obtain the resultant velocity in discretization method by staggered grid. The result of this study can help users to write their own codes and use commercial CFD codes successfully in solving equations of fluid flow using numerical discretization schemes.

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.*, **88**, 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] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta and J. J. C. De Santanna, "Internet of Things in healthcare: Interoperability and security issues," in 2012 IEEE international conference on communications (ICC)., 2012.
- [4] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Survey on Blockchain for Internet of Things," *Computer Communications.*, 2019.
- [5] 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.*, **3**, 678-708(2015).
- [6] Z. Pang, "Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being," 2013.
- [7] 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.*, **2**, 515-526 (2015).
- [8] 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.*, **140**, 1-22(2019).
- [9] 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.
- [10] 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*., **43**, 74-86 (2015).
- [11] G. Xiao, J. Guo, L. Da Xu and Z. Gong, "User interoperability with heterogeneous IoT devices through transformation," *IEEE Transactions on Industrial Informatics*., **10**, 1486-1496, 2014.
- [12] 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*., **81**, 111-124(2017).
- [13] Y. Yang, X. Zheng and C. Tang, "Lightweight distributed secure data management system for health internet of things," *Journal of Network and Computer Applications*., **89**, 26-37(2017).
- [14] D. Androcec and N. Vrcek, "Thing as a service interoperability: review and framework proposal," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)., 2016.
- [15] 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.
- [16] N. Abdullah, A. Hakansson and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)., 2017.
- [17] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)., 2016.
- [18] T.-T. Kuo, H.-E. Kim and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*., **24**, 1211-1220 (2017).
- [19] A. Gyrard, M. Serrano and G. A. Atemezeng, "Semantic web methodologies, best practices and ontology engineering applied to Internet of Things," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)., 2015.
- [20] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "Medrec: Using Blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD)., 2016.
- [21] M. Blackstock and R. Lea, "IoT interoperability: A hub-based approach," in 2014 international conference on the internet of things (IOT)., 2014.
- [22] M. A. Jarwar, S. Ali and I. Chong, "Exploring web objects enabled data-driven microservices for E-health service provision in IoT environment," in 2018 International Conference on Information and Communication Technology Convergence (ICTC)., 2018.
- [23] J. Strassner and W. W. Diab, "A semantic interoperability architecture for Internet of Things data sharing and computing," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016.
- [24] P. Desai, A. Sheth and P. Anantharam, "Semantic gateway as a service architecture for iot interoperability," in 2015 IEEE International Conference on Mobile Services., 2015.
- [25] V. Curcin, H. Bastiaens and A. Taweel, "Clinical Data Integration Model: Core Interoperability Ontology for Research Using Primary Care Data".
- [26] S. I. Khan and A. S. L. Hoque, "Privacy and security problems of national health data warehouse: a convenient solution for developing countries," in 2016 International Conference on Networking Systems and Security (NSysS), 2016.
- [27] A. Stanciu, "Blockchain based distributed control system for edge computing," in 2017 21st International Conference on Control Systems and Computer Science (CSCS)., 2017.
- [28] J. Huang and M. S. Fox, "An ontology of trust: formal semantics and transitivity," in *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, 2006.
- [29] 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*., **78**, 217-225(2017).
- [30] J.-F. Ethier, V. Curcin, A. Barton, M. M. McGilchrist, H. Bastiaens, A. Andreasson, J. Rossiter, L. Zhao, T. N. Arvanitis, A. Taweel and others, "Clinical data integration model," *Methods of information in medicine*., **54**, 16-23

(2015).

- [31] J. B. Bernabe, J. L. H. Ramos and A. F. S. Gomez, "TACIoT: multidimensional trust-aware access control system for the Internet of Things," *Soft Computing.*, **20**, 1763-1779(2016).
- [32] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications.*, 2019.
- [33] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed and M. Imran, "Securing IoTs in distributed Blockchain: Analysis, requirements and open issues," *Future Generation Computer Systems.*, **100**, 325-343(2019).
- [34] Y. Lu, "The Blockchain: State-of-the-Art and Research Challenges," *Journal of Industrial Information Integration*, 2019.
- [35] M. A. Khan and K. Salah, "IoT security: Review, Blockchain solutions, and open challenges," *Future Generation Computer Systems.*, **82**, 395-411(2018).
- [36] M. Banerjee, J. Lee and K.-K. R. Choo, "A Blockchain future for internet of things security: A position paper," *Digital Communications and Networks.*, **4**, 149-160(2018).
- [37] 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.
- [38] 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.
- [39] 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.
- [40] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems.*, **95**, 420-429 (2019).
- [41] 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.*, **95**, 511-521(2019).
- [42] 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.*, **9**, 5665(2018).